vSphere Update Manager Installation and Administration Guide

17 APR 2018

VMware vSphere 6.7

vSphere Update Manager 6.7



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Installing and Administering VMware vSphere Update Manager

Installing and Administering VMware vSphere Update Manager provides information about installing, configuring, and using VMware® vSphere Update Manager to scan and remediate the objects in your vSphere environment. It also describes the tasks that you can perform to update your vSphere inventory objects and make them compliant against attached baselines and baseline groups.

For scanning and remediation, Update Manager works with the following ESXi versions:

- For VMware Tools and virtual machine hardware upgrade operations, Update Manager works with 6.0, ESXi 6.5, and ESXi 6.7.
- For ESXi host patching operations, Update Manager works with ESXi 6.0, ESXi 6.5, and ESXi 6.7.
- For ESXi host upgrade operations, Update Manager works withESXi 6.0, ESXi 6.5, and their respective Update releases.

Intended Audience

This information is intended for anyone who wants to install, upgrade, migrate, or use Update Manager. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

vSphere Client and vSphere Web Client

Instructions in this guide reflect the vSphere Client (an HTML5-based GUI). You can also use the instructions to perform most of the tasks by using the vSphere Web Client (a Flex-based GUI).

Tasks for which the workflow differs significantly between the vSphere Client and the vSphere Web Client have duplicate procedures that provide steps according to the respective client interface. The procedures that relate to the vSphere Web Client, contain vSphere Web Client in the title.

VMware Glossary

VMware provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Understanding Update Manager 1

Update Manager enables centralized, automated patch and version management for VMware vSphere and offers support for VMware ESXi hosts, and virtual machines.

With Update Manager, you can perform the following tasks:

- Upgrade and patch ESXi hosts.
- Install and update third-party software on hosts.
- Upgrade virtual machine hardware and VMware Tools.

Update Manager requires network connectivity with VMware vCenter Server. Each installation of Update Manager must be associated (registered) with a single vCenter Server instance.

The Update Manager module consists of a server component and of a client component.

You can use Update Manager with either vCenter Server that runs on Windows or with the vCenter Server Appliance.

If you want to use Update Manager with vCenter Server, you have to perform Update Manager installation on a Windows machine. You can install the Update Manager server component either on the same Windows server where the vCenter Server is installed or on a separate machine. To install Update Manager, you must have Windows administrator credentials for the computer on which you install Update Manager.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, and you want to use Update Manager for each vCenter Server system, you must install and register Update Manager instances with each vCenter Server system. You can use an Update Manager instance only with the vCenter Server system with which it is registered.

From vSphere 6.5 and later, it is no longer supported to register Update Manager to a vCenter Server Appliance during the installation of the Update Manager server on a Windows machine.

The vCenter Server Appliance delivers Update Manager as a service. Update Manager is bundled in the vCenter Server Appliance.

The Update Manager client component is a plug-in that runs on the vSphere Web Client (Flex) and the vSphere Client (HTML5). The Update Manager client component is automatically enabled after installation of the Update Manager server component on Windows, and after deployment of the vCenter Server Appliance.

However, if you are using Update Manager server that runs on Windows, you can see the Update Manager client component only in the vSphere Web Client. If you are using Update Manager with the vCenter Server Appliance, the Update Manager client component is available in both the vSphere Web Client and the vSphere Client.

You can deploy Update Manager in a secured network without Internet access. In such a case, you can use the VMware vSphere Update Manager Download Service (UMDS) to download update metadata and update binaries.

This chapter includes the following topics:

- Overview of the Update Manager Client Interfaces
- About the Update Manager Process

Overview of the Update Manager Client Interfaces

The Update Manager server has a client interface for the vSphere Web Client and the vSphere Client.

The Update Manager client interfaces do not require any installation, and are automatically enabled in the vSphere Web Client and the vSphere Client after you install the Update Manager server component on Windows, or deploy the vCenter Server Appliance.

When you use an Update Manager server instance that runs on Windows, you can use Update Manager only with the vSphere Web Client. The vSphere Client does not support using Update Manager server that runs on Windows and is connected to a vCenter Server instance that also runs on Windows. To use Update Manager capabilities with the vSphere Client, use a vCenter Server Appliance where Update Manager runs as a service.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, and you have installed and registered more than one Update Manager instance, you can configure the settings for each Update Manager instance. Configuration properties that you modify are applied only to the Update Manager instance that you specify and are not propagated to the other instances in the group. You can specify an Update Manager instance by selecting the name of the vCenter Server system with which the Update Manager instance is registered from the navigation bar. In vSphere 6.7, you can make configuration changes only by using the Update Manager client interface in the vSphere Web Client.

For a vCenter Server system that is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can also manage baselines and baseline groups as well as scan and remediate only the inventory objects managed by the vCenter Server system with which Update Manager is registered.

The Update Manager client interface have two main views, administration view and compliance view.

- Update Manager Client Interface in the vSphere Client

  In the vSphere Client, the Update Manager client interface appears as tab **Updates**. The **Updates** tab is a first-level tab and is last in the row of first-level tabs, following the **Summary**, the **Monitor**, the **Configure**, the **Permissions**, and so on, tabs.

- Update Manager Client Interface in the vSphere Web Client

  In the vSphere Web Client, the Update Manager client interface appears as tab **Update Manager**. The **Update Manager** tab is a first-level tab and is last in the row of first-level tabs, following the **Summary**, the **Monitor**, the **Configure**, the **Permissions**, and so on, tabs.

Update Manager Client Interface in the vSphere Client

In the vSphere Client, the Update Manager client interface appears as tab **Updates**. The **Updates** tab is a first-level tab and is last in the row of first-level tabs, following the **Summary**, the **Monitor**, the **Configure**, the **Permissions**, and so on, tabs.

In the Update Manager administration view in the vSphere Client, you have the following top-level tabs: **Home**, **Baselines**, **Updates**, and **ESXi Images**.

Under each respective tab, you can perform the following tasks:

- See statistics about non-compliant host and clusters in your vSphere environment.
- Create and manage baselines and baseline groups.
- Review the patch repository.
- Import ESXi images.

To access the Update Manager compliance view in the vSphere Client, selected an inventory object such as a data center, a cluster, or a host and click the **Updates** tab.

In the Update Manager compliance view, you can do the following tasks:

- Check compliance and scan results for hosts and clusters.
- Attach and detach baselines and baseline groups to hosts and clusters.
- Generate a pre-check remediation report that lists recommended actions to ensure successful remediation.
- Stage patches or extensions to hosts.
- Remediate hosts against patch, extension, and upgrade baselines. (Changing the default host and cluster settings during remediation is not supported in vSphere 6.7).
- Remediate hosts that are part of a vSAN cluster against system-managed baselines.

Remediation operations of virtual machines are not supported with the vSphere Client 6.7. Use the vSphere Web Client to upgrade VMware Tools and the hardware version of the virtual machines in your vSphere environment.

Update Manager Client Interface in the vSphere Web Client

In the vSphere Web Client, the Update Manager client interface appears as tab **Update Manager**. The **Update Manager** tab is a first-level tab and is last in the row of first-level tabs, following the **Summary**, the **Monitor**, the **Configure**, the **Permissions**, and so on, tabs.

To see the Update Manager client interface in the vSphere Web Client, you must have the **View Compliance Status** privilege.

To access the Update Manager administration view in the vSphere Web Client, click the vSphere Web Client **Home** menu, and click **Update Manager**. From the **Objects** tab, click the IP Address of the Update Manager instance you want to administer. Another way to navigate to the Update Manager administration view is to click **Go to Admin View** while you are in the Update Manager compliance view.

In the Update Manager administration view in the vSphere Web Client, you have the following top-level tabs: **Getting Started**, **Monitor**, and **Manage**.

Under the **Monitor** tab, you can perform the following tasks:

- View Update Manager events
- Review and check notifications

Under the **Manage** tab, you can perform the following tasks:

- Configure the Update Manager settings.
- Create and manage baselines and baseline groups.
- Review the patch repository.
- Import ESXi images.

To access the Update Manager compliance view in the vSphere Web Client, selected an inventory object such as a data center, a cluster, a host, a VM, a vApp, and click the **Update Manager** tab.

In the Update Manager compliance view, you can do the following tasks:

- View compliance and scan results for each selected inventory object
- Attach and detach baselines and baseline groups from a selected inventory object.
- Scan a selected inventory object.
- Stage patches or extensions to hosts
- Remediate hosts against patch, extension, and upgrade baselines
- Remediate hosts that are part of a vSAN cluster against system-managed baselines

About the Update Manager Process

Upgrading vSphere objects and applying patches or extensions with Update Manager is a multistage process in which procedures must be performed in a particular order. Following the suggested process helps ensure a smooth update with a minimum of system downtime.

The Update Manager process begins by downloading information (metadata) about a set of patches and extensions. One or more of these patches or extensions are aggregated to form a baseline. You can add multiple baselines to a baseline group. A baseline group is a composite object that consists of a set of nonconflicting baselines. You can use baseline groups to combine different types of baselines, and scan and remediate an inventory object against all of them as a whole. If a baseline group contains both upgrade and patch or extension baselines, the upgrade runs first.

A collection of virtual machines and ESXi hosts or individual inventory objects can be scanned for compliance with a baseline or a baseline group and later remediated. You can initiate these processes manually or through scheduled tasks.

- Configuring the Update Manager Download Source

  You can configure the Update Manager server to download patches and extensions either from the Internet or from a shared repository. You can also import patches and extensions manually from a ZIP file.

- Downloading Updates and Related Metadata

  Downloading host patches, extensions, and related metadata is a predefined automatic process that you can modify. By default, at regular configurable intervals, Update Manager contacts VMware or third-party sources to gather the latest information (metadata) about available upgrades, patches, or extensions.

- Importing ESXi Images

  You can upgrade the hosts in your environment to ESXi 6.7 by using host upgrade baselines. To create a host upgrade baseline, you must first upload at least one ESXi 6.7 `.iso` image to the Update Manager repository.

- Creating Baselines and Baseline Groups

  Baselines contain a collection of one or more patches, extensions, service packs, bug fixes, or upgrades, and can be classified as patch, extension, or upgrade baselines. Baseline groups are assembled from existing baselines.

- Attaching Baselines and Baseline Groups to vSphere Objects

  To use baselines and baseline groups, you must attach them to selected inventory objects such as container objects, virtual machines, or hosts.

- Scanning Selected vSphere Objects

  Scanning is the process in which attributes of a set of hosts or virtual machines are evaluated against all patches, extensions, and upgrades from an attached baseline or baseline group, depending on the type of scan you select.

- Reviewing Scan Results

  Update Manager scans vSphere objects to determine how they comply with baselines and baseline groups that you attach. You can filter scan results by text search, group selection, baseline selection, and compliance status selection.

- Staging Patches and Extensions to Hosts

  You can stage patches and extensions before remediation to ensure that the patches and extensions are downloaded to the host. Staging patches and extensions is an optional step that can reduce the time during which hosts are in maintenance mode.

- Remediating Selected vSphere Objects

  Remediation is the process in which Update Manager applies patches, extensions, and upgrades to ESXi hosts and virtual machines after a scan is complete.

Configuring the Update Manager Download Source

You can configure the Update Manager server to download patches and extensions either from the Internet or from a shared repository. You can also import patches and extensions manually from a ZIP file.

Configuring the Update Manager download source is an optional step.

If your deployment system is connected to the Internet, you can use the default settings and links for downloading upgrades, patches, and extensions to the Update Manager repository. You can also add URL addresses to download third-party patches and extensions. Third-party patches and extensions are applicable only to hosts that are running ESXi 6.0 and later.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the upgrades, patches, and extensions by using Update Manager Download Service (UMDS).

For more information about UMDS, see Chapter 6 Installing, Setting Up, and Using Update Manager Download Service.

With Update Manager, you can import both VMware and third-party patches or extensions manually from a ZIP file, also called an offline bundle. Import of offline bundles is supported only for hosts that are running ESXi 6.0 and later. You download the offline bundle ZIP files from the Internet or copy them from a media drive, and save them on a local or a shared network drive. You can import the patches or extensions to the Update Manager patch repository later. You can download offline bundles from the VMware Web site or from the Web sites of third-party vendors.

Note You can use offline bundles for host patching operations only. You cannot use third-party offline bundles or offline bundles that you generated from custom VIB sets for host upgrade from ESXi 6.0 and ESXi 6.5 to ESXi 6.7.

For detailed descriptions of the procedures, see Configuring the Update Manager Download Sources.

Downloading Updates and Related Metadata

Downloading host patches, extensions, and related metadata is a predefined automatic process that you can modify. By default, at regular configurable intervals, Update Manager contacts VMware or third-party sources to gather the latest information (metadata) about available upgrades, patches, or extensions.

VMware provides information about patches for ESXi hosts.

Update Manager downloads the following types of information:

- Metadata about all ESXi 6.x patches regardless of whether you have hosts of such versions in your environment.
- Metadata about ESXi 6.x patches as well as about extensions from third-party vendor URL addresses.
- Notifications, alerts, and patch recalls for ESXi 6.x hosts.

Downloading information about all updates is a relatively low-cost operation in terms of disk space and network bandwidth. The availability of regularly updated metadata lets you add scanning tasks on the hosts at any time.

Update Manager supports the recall of patches for hosts that are running ESXi 6.0 or later. A patch is recalled if the released patch has problems or potential issues. After you scan the hosts in your environment, Update Manager alerts you if the recalled patch has been installed on a certain host. Recalled patches cannot be installed on hosts with Update Manager. Update Manager also deletes all the recalled patches from the Update Manager patch repository. After a patch fixing the problem is released, Update Manager downloads the new patch to its patch repository. If you have already installed the problematic patch, Update Manager notifies you that a fix was released and prompts you to apply the new patch.

If Update Manager cannot download upgrades, patches, or extensions—for example, if it is deployed on an internal network segment that does not have Internet access—you must use UMDS to download and store the data on the machine on which UMDS is installed. The Update Manager server can use the upgrades, patches, and extensions that UMDS downloaded after you export them.

For more information about UMDS, see Chapter 6 Installing, Setting Up, and Using Update Manager Download Service.

You can configure Update Manager to use an Internet proxy to download upgrades, patches, extensions, and related metadata.

You can change the time intervals at which Update Manager downloads updates or checks for notifications. For detailed descriptions of the procedures, see Configure Checking for Updates and Configure Notifications Checks.

Types of Software Updates and Related Terms

Update Manager downloads software updates and metadata from Internet depots or UMDS-created shared repositories. You can import offline bundles and host upgrade images from a local storage device into the local Update Manager repository.

Bulletin
A grouping of one or more VIBs. Bulletins are defined within metadata.

Depot
A logical grouping of VIBs and associated metadata that is published online.

Host upgrade image
An ESXi image that you can import in the Update Manager repository and use for upgrading ESXi 6.0 or ESXi 6.5 hosts to ESXi 6.7.

Extension
A bulletin that defines a group of VIBs for adding an optional component to an ESXi host. An extension is usually provided by a third party that is also responsible for patches or updates to the extension.

Metadata
Extra data that defines dependency information, textual descriptions, system requirements, and bulletins.

Offline bundle ZIP — An archive that encapsulates VIBs and corresponding metadata in a self-contained package that is useful for offline patching. You cannot use third-party offline bundles or offline bundles that you generated from custom VIB sets for host upgrade from ESXi 6.0 or ESXi 6.5 to ESXi 6.7.

Patch — A bulletin that groups one or more VIBs together to address a particular issue or enhancement.

Roll-up — A collection of patches that is grouped for ease of download and deployment.

VIB — A VIB is a single software package.

Importing ESXi Images

You can upgrade the hosts in your environment to ESXi 6.7 by using host upgrade baselines. To create a host upgrade baseline, you must first upload at least one ESXi 6.7 `.iso` image to the Update Manager repository.

With Update Manager 6.7 you can upgrade hosts that are running ESXi 6.0 or ESXi 6.5 to ESXi 6.7. Host upgrades to ESXi 5.x, ESXi 6.0 or ESXi 6.5 are not supported.

Before uploading ESXi images, obtain the image files from the VMware Web site or another source. You can create custom ESXi images that contain third-party VIBs by using vSphere ESXi Image Builder. For more information, see *Customizing Installations with vSphere ESXi Image Builder*.

You can upload and manage ESXi images from the **ESXi Images** tab of the Update Manager Administration view.

ESXi images that you import are kept in the Update Manager repository. You can include ESXi images in host upgrade baselines. To delete an ESXi image from the Update Manager repository, first you must delete the upgrade baseline that contains it. After you delete the baseline, you can delete the image from the **ESXi Images** tab.

For more information about importing ESXi images and creating host upgrade baselines, see Create a Host Upgrade Baseline in the vSphere Web Client.

Creating Baselines and Baseline Groups

Baselines contain a collection of one or more patches, extensions, service packs, bug fixes, or upgrades, and can be classified as patch, extension, or upgrade baselines. Baseline groups are assembled from existing baselines.

Host baseline groups can contain a single upgrade baseline, and various patch and extension baselines.

Virtual machine baseline groups can contain up to two upgrade baselines: one VMware Tools upgrade baseline, and one virtual machine hardware upgrade baseline.

When you scan hosts and virtual machines, you evaluate them against baselines and baseline groups to determine their level of compliance.

Update Manager includes two predefined patch baselines and two predefined upgrade baselines. You cannot edit or delete the predefined virtual machine baselines. You can use the predefined baselines, or create patch, extension, and upgrade baselines that meet your criteria. Baselines you create, and predefined baselines, can be combined in baseline groups. For more information about creating and managing baselines and baseline groups, see Chapter 7 Working with Baselines and Baseline Groups.

Baseline Types

Update Manager supports different types of baselines that you can use when scanning and remediating objects in your inventory.

Update Manager provides upgrade, patch, and extension baselines.

Upgrade Baselines

Baseline	Description
Host Upgrade Baseline	Defines to which version to upgrade the hosts in your environment. With Update Manager 6.7, you can upgrade ESXi hosts from version 6.0 and 6.5 to ESXi 6.7.
Virtual Machine Upgrade Baseline	Defines to which version to upgrade virtual hardware or VMware Tools. With Update Manager 6.7 you can upgrade to hardware version vmx-14 and to the latest VMware Tools version on hosts that are running ESXi 6.7.

Patch Baselines

Patch baselines define a number of patches that must be applied to a given host. Patch baselines can be either dynamic or fixed.

Baseline	Description
Dynamic Patch Baseline	The contents of a dynamic baseline are based on available patches that meet the specified criteria. As the set of available patches changes, dynamic baselines are updated as well. You can explicitly include or exclude any patches.
Fixed Patch Baseline	You manually specify which patches to include in the fixed patch baseline from the total set of patches available in the Update Manager repository.

Extension Baselines

Baseline	Description
Extension Baseline	Contains extensions (additional software such as third-party device drivers) that must be applied to a given host. Extensions are installed on hosts that do not have such software installed on them, and patched on hosts that already have the software installed. All third-party software for ESXi hosts is classified as a host extension, although host extensions are not restricted to just third-party software.

Update Manager Default Baselines

Update Manager includes default baselines that you can use to scan any virtual machine or host to determine whether the hosts in your environment are updated with the latest patches, or whether the virtual machines are upgraded to the latest version.

Critical Host Patches (Predefined)
Checks ESXi hosts for compliance with all critical patches.

Non-Critical Host Patches (Predefined)
Checks ESXi hosts for compliance with all optional patches.

VMware Tools Upgrade to Match Host (Predefined)
Checks virtual machines for compliance with the latest VMware Tools version on the host. Update Manager supports upgrading of VMware Tools for virtual machines on hosts that are running ESXi 6.0.x and later.

VM Hardware Upgrade to Match Host (Predefined)
Checks the virtual hardware of a virtual machine for compliance with the latest version supported by the host. Update Manager supports upgrading to virtual hardware version vmx-14 on hosts that are running ESXi 6.7.

Baseline Groups

Baseline groups can contain patch, extension, and upgrade baselines. The baselines that you add to a baseline group must be non-conflicting.

A baseline group is limited to a combination of patches, extensions, and upgrades. The following are valid combinations of baselines that can make up a baseline group:

- Multiple host patch and extension baselines.
- One upgrade baseline, multiple patch and extension baselines.

  For example, one ESXi upgrade baseline and multiple ESXi patch or extension baselines.
- Multiple upgrade baselines, but only one upgrade baseline per upgrade type (like VMware Tools, virtual machine hardware, or host).

  For example, VMware Tools Upgrade to Match Host baseline and VM Hardware Upgrade to Match Host baseline.

Attaching Baselines and Baseline Groups to vSphere Objects

To use baselines and baseline groups, you must attach them to selected inventory objects such as container objects, virtual machines, or hosts.

Although you can attach baselines and baseline groups to individual objects, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and data centers. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

For a detailed description of the procedure, see Attach Baselines and Baseline Groups to Objects in the vSphere Web Client.

Scanning Selected vSphere Objects

Scanning is the process in which attributes of a set of hosts or virtual machines are evaluated against all patches, extensions, and upgrades from an attached baseline or baseline group, depending on the type of scan you select.

You can scan a host installation to determine whether the latest patches or extensions are applied, or you can scan a virtual machine to determine whether it is up to date with the latest virtual hardware or VMware Tools version.

Update Manager supports the following types of scan:

Host patch scan You can perform patch scans on ESXi 6.0 and later.

Host extensions scan You can scan ESXi 6.0 and later for extensions (additional software modules).

Host upgrade scan You can scan ESXi 6.0 and ESXi 6.5 for upgrading to ESXi 6.5.

VMware Tools scan You can scan virtual machines running Windows or Linux for the latest VMware Tools version. You can perform VMware Tools scans on online or offline virtual machines and templates. You must power on the virtual machine at least once before performing a VMware Tools scan.

Virtual machine hardware upgrade scan You can scan virtual machines running Windows or Linux for the latest virtual hardware supported on the host. You can perform hardware-upgrade scans on online or offline virtual machines and templates.

You can use VMware Studio 2.0 and later to automate the creation of ready-to-deploy vApps with pre-populated application software and operating systems. VMware Studio adds a network agent to the guest so that vApps bootstrap with minimal effort. Configuration parameters specified for vApps appear as OVF properties in the vCenter Server deployment wizard. For more information about VMware Studio, see the VMware SDK and API documentation for VMware Studio. For more information about vApp, you can also check the VMware blog site. You can download VMware Studio from the VMware website.

You can initiate scans on container objects, such as data centers, clusters, or folders, to scan all the ESXi hosts or virtual machines in that container object.

You can configure Update Manager to scan virtual machines and ESXi hosts against baselines and baseline groups by manually initiating or scheduling scans to generate compliance information. Schedule scan tasks at a data center or vCenter Server system level to make sure that scans are up to date.

For manual and scheduled scanning procedures, see Chapter 8 Scanning vSphere Objects and Viewing Scan Results.

Reviewing Scan Results

Update Manager scans vSphere objects to determine how they comply with baselines and baseline groups that you attach. You can filter scan results by text search, group selection, baseline selection, and compliance status selection.

When you select a container object, you view the overall compliance status of the container against the attached baselines as a group. You also see the individual compliance statuses of the objects in the selected container against all baselines. If you select an individual baseline attached to the container object, you see the compliance status of the container against the selected baseline.

If you select an individual virtual machine, appliance, or host, you see the overall compliance status of the selected object against all attached baselines and the number of updates. If you select an individual baseline attached to this object, you see the number of updates grouped by the compliance status for that baseline.

The compliance information is displayed on the **Update Manager** tab. For more information about viewing compliance information, see Viewing Scan Results and Compliance States for vSphere Objects.

Staging Patches and Extensions to Hosts

You can stage patches and extensions before remediation to ensure that the patches and extensions are downloaded to the host. Staging patches and extensions is an optional step that can reduce the time during which hosts are in maintenance mode.

Staging patches and extensions to hosts that are running ESXi 5.0 or later lets you download the patches and extensions from the Update Manager server to the ESXi hosts without applying the patches or extensions immediately. Staging patches and extensions speeds up the remediation process because the patches and extensions are already available locally on the hosts.

Important Update Manager can stage patches to PXE booted ESXi hosts.

For more information about staging patches, see Stage Patches and Extensions to ESXi Hosts in the vSphere Web Client.

Remediating Selected vSphere Objects

Remediation is the process in which Update Manager applies patches, extensions, and upgrades to ESXi hosts and virtual machines after a scan is complete.

Remediation makes the selected vSphere objects compliant with patch, extension, and upgrade baselines.

As with scanning, you can remediate single hosts or virtual machines. You can also initiate remediation on a folder, a cluster, or a data center level.

Update Manager supports remediation for the following inventory objects:

- Powered on, suspended, or powered off virtual machines and templates for VMware Tools and virtual machine hardware upgrade.

- ESXi hosts for patch, extension, and upgrade remediation.

You can remediate the objects in your vSphere inventory by using either manual remediation or scheduled remediation. For more information about manual and scheduled remediation, see Chapter 9 Remediating vSphere Objects.

Remediating Hosts

Update Manager 6.7 supports upgrade from ESXi 6.0.x and ESXi 6.5.x to ESXi 6.7.

Important If you enable the setting from the **ESX Host/Cluster Settings** page of the **Configuration** tab, or from the **Remediate** wizard, you can patch PXE booted ESXi hosts.

After you upload ESXi images, upgrades for ESXi hosts are managed through baselines and baseline groups.

Typically, if the update requires it, hosts are put into maintenance mode before remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure a consistent user experience, vCenter Server migrates the virtual machines to other hosts within a cluster before the host is put in maintenance mode. vCenter Server can migrate the virtual machines if the cluster is configured for vMotion and if VMware Distributed Resource Scheduler (DRS) and VMware Enhanced vMotion Compatibility (EVC) are enabled. EVC is not a prerequisite for vMotion. EVC guarantees that the CPUs of the hosts are compatible. For other containers or individual hosts that are not in a cluster, migration with vMotion cannot be performed.

Important After you have upgraded your host to ESXi 6.7, you cannot roll back to your version ESXi 6.0.x or ESXi 6.5.x software. Back up your host configuration before performing an upgrade. If the upgrade fails, you can reinstall the ESXi 6.0.x or ESXi 6.5.x software that you upgraded from, and restore your host configuration. For more information about backing up and restoring your ESXi configuration, see *vSphere Upgrade*.

Remediation of ESXi 6.0 and 6.5 hosts to their respective ESXi update releases is a patching process, while the remediation of ESXi hosts from version 6.0 or 6.5 to 6.7 is an upgrade process.

Remediating Virtual Machines

You can upgrade VMware Tools, and the virtual hardware of virtual machines to a later version. Upgrades for virtual machines are managed through the Update Manager default virtual machine upgrade baselines.

Orchestrated Upgrades

With Update Manager, you can perform orchestrated upgrades of hosts and virtual machines. With orchestrated upgrades, you can upgrade hosts and virtual machines in your vSphere inventory by using baseline groups.

You can perform an orchestrated upgrade of hosts by using a baseline group that contains a single host upgrade baseline and multiple patch or extension baselines. Update Manager first upgrades the hosts and then applies the patch or extension baselines.

You can perform an orchestrated upgrade of virtual machines by using a virtual machine baseline group that contains the following baselines:

- VM Hardware Upgrade to Match Host
- VMware Tools Upgrade to Match Host

You can use orchestrated upgrades to upgrade the virtual hardware and VMware Tools of virtual machines in the inventory at the same time. The VMware Tools upgrade baseline runs first, followed by the virtual machine hardware upgrade baseline.

Orchestrated upgrades can be performed at a cluster, folder, or a data center level.

Installing, Upgrading, and Uninstalling Update Manager on a Windows Operating System 2

You can install Update Manager server on a Windows virtual or physical machine and connect it to a vCenter Server instance that also runs on Windows. You can later uninstall the Update Manager server. If you are running Update Manager server of an earlier version, you can upgrade it to version 6.7.

- System Requirements

  To run and use the Update Manager server, you must ensure that your environment satisfies certain conditions. You also must ensure that the vCenter Server and Update Manager are of compatible versions.

- Preparing the Update Manager Database

  The Update Manager server and Update Manager Download Service (UMDS) that you install on Windows require a database to store and organize server data. Update Manager supports Oracle, Microsoft SQL Server databases.

- Installing Update Manager on Windows

  The Update Manager server is a 64-bit application. You can install the Update Manager server for Windows only on 64-bit Windows machines.

- Upgrading Update Manager that Runs on Windows

  You can upgrade to Update Manager 6.7 only from Update Manager versions 6.0 or 6.5 that are installed on a 64-bit Windows operating system.

- Uninstalling Update Manager that Runs on Windows

  Update Manager has a relatively small impact on computing resources such as disk space. Unless you are certain that you want to remove Update Manager, leave an existing installation in place.

- Best Practices and Recommendations for Update Manager Environment

  You can install Update Manager on the server on which vCenter Server runs or on a different server.

System Requirements

To run and use the Update Manager server, you must ensure that your environment satisfies certain conditions. You also must ensure that the vCenter Server and Update Manager are of compatible versions.

Before you install Update Manager on Windows, you must set up an Oracle or Microsoft SQL Server database. If your deployment is relatively small and contains up to 5 hosts and 50 virtual machines, you can use the bundled Microsoft SQL Server 2012 Express database, which you can select to install from the Update Manager installation wizard.

You can install Update Manager on a physical server or on a virtual machine. You can install the Update Manager server component on the same Windows machine as vCenter Server or on a different machine. After you install the Update Manager server component, to use Update Manager, the Update Manager client is automatically enabled on the vSphere Web Client.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can install and register Update Manager instances with each vCenter Server system.

Update Manager Hardware Requirements

You can run Update Manager on any system that meets the minimum hardware requirements.

Minimum hardware requirements for Update Manager vary depending on how Update Manager is deployed. If the database is installed on the same machine as Update Manager, requirements for memory size and processor speed are higher. To ensure acceptable performance, verify that your system meets the minimum hardware requirements.

Table 2-1. Minimum Hardware Requirements

Hardware	Requirements
Processor	Intel or AMD x86 processor with two or more logical cores, each with a speed of 2GHz
Network	10/100 Mbps
	For best performance, use a Gigabit connection between Update Manager and the ESXi hosts
Memory	2GB RAM if Update Manager and vCenter Server are on different machines
	8GB RAM if Update Manager and vCenter Server are on the same machine

Update Manager uses a SQL Server or Oracle database. You should use a dedicated database for Update Manager, not a database shared with vCenter Server, and should back up the database periodically. Best practice is to have the database on the same computer as Update Manager or on a computer in the local network.

Depending on the size of your deployment, Update Manager requires a minimum amount of free space per month for database usage. For more information about space requirements, see the *VMware vSphere Update Manager Sizing Estimator*.

Supported Windows Operating Systems and Database Formats

Update Manager works with specific databases and operating systems.

The Update Manager server requires a 64-bit Windows system.

To see a list of the supported Windows operating systems on which you can install the Update Manager server and the UMDS, see Supported host operating systems for VMware vCenter Server installation. The supported Windows operating systems for vCenter Server installation listed in the article also apply for installation of the respective versions of the Update Manager server and the UMDS.

Note Make sure the Windows system on which you are installing the Update Manager server is not an Active Directory domain controller.

The Update Manager server that you install on Windows requires a SQL Server or an Oracle database. Update Manager can handle small-scale environments using the bundled in the installer SQL Server 2012 Express database. For environments with more than 5 hosts and 50 virtual machines, create either an Oracle or a SQL Server database for Update Manager. For large-scale environments, set up the Update Manager database on a different computer than the Update Manager server and the vCenter Server database.

To see a list of database formats that are compatible with the Update Manager server and the UMDS, select the **Solution/Database Interoperability** option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Update Manager Compatibility with vCenter Server , vCenter Server Appliance , vSphere Web Client , and vSphere Client

Update Manager 6.7 is compatible only with vCenter Server 6.7 and its components.

An Update Manager server that runs on Windows is only compatible with the vCenter Server that runs on Windows and the vSphere Web Client.

The vCenter Server Appliance is packed with the Update Manager server, and after deployment runs Update Manager as a service. The vCenter Server Appliance supports Update Manager client interfaces in both the vSphere Client and the vSphere Web Client.

There are differences in the Update Manager user interface between the vSphere Client and the vSphere Web Client. For example, in the vSphere Client you are unable to change Update Manager configuration settings, or change default remediation options in the remediation wizard, or remediate VMs. For such operations, use the vSphere Web Client.

Required Database Privileges

The set of database privileges needed for the Update Manager installation and upgrade differs from the set of privileges needed for the Update Manager administration.

Before installing or upgrading Update Manager, you must grant adequate privileges to the database user.

Table 2-2. Database Privileges Needed for Installation or Upgrade of Update Manager

Database	Privileges
Oracle	Either assign the DBA role, or grant the following set of privileges to the Update Manager Oracle database user. ■ **connect** ■ **execute on dbms_lock** ■ **create view** ■ **create procedure** ■ **create table** ■ **create sequence** ■ **create any sequence** ■ **create any table** ■ **create type** ■ **unlimited tablespace**
Microsoft SQL Server	Make sure that the database user has either a **sysadmin** server role or the **db_owner** fixed database role on the Update Manager database and the MSDB database. Although the **db_owner** role is required for the upgrade, SQL jobs are not created as part of the Update Manager installation or upgrade.

To run Update Manager, you must grant a set of minimum privileges to the database user.

Table 2-3. Database Privileges Needed for Using Update Manager

Database	Privileges
Oracle	The minimum required privileges of the Oracle database user are the following: ■ **create session** ■ **create any table** ■ **drop any table**
Microsoft SQL Server	The database user must have either a **sysadmin** server role or the **db_owner** fixed database role on the Update Manager database and the MSDB database.

Preparing the Update Manager Database

The Update Manager server and Update Manager Download Service (UMDS) that you install on Windows require a database to store and organize server data. Update Manager supports Oracle, Microsoft SQL Server databases.

Before installing the Update Manager server on a Windows machine, you must create a database instance and configure it to ensure that all Update Manager database tables can be created in it. You can install and configure the Microsoft SQL Server 2012 Express database that is embedded with Update Manager. Microsoft SQL Server 2012 Express is recommended for small deployments of up to 5 hosts and 50 virtual machines.

Update Manager 6.7 server is a 64-bit application, and you can install it only on 64-bit machines. Update Manager requires a 64-bit DSN.

To use Microsoft SQL Server and Oracle databases, you must configure a 64-bit system DSN and test it with ODBC.

The Update Manager database you use can be the same as the vCenter Server database. You can also use a separate type of database, or you can use existing database clusters. For optimal results in a large-scale environment, use a dedicated Update Manager database that runs on a different machine than the vCenter Server system database.

The Update Manager server requires administrative credentials to connect to the database. If the database user name and password change after you install the Update Manager server or UMDS on Windows, you can reconfigure Update Manager and UMDS without the need to reinstall them. See the *Reconfiguring VMware vSphere Update Manager* documentation.

Before you begin the database setup, review the supported databases. If you create an ODBC connection to a database server that is not supported, a DSN for the unsupported database might be displayed in the drop-down menu of the Update Manager installation wizard. For more information about the supported database patches, see the Solution/Database Interoperability option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. If you do not prepare your database correctly, the Update Manager installer might display error or warning messages.

Create a 64-Bit DSN

The Update Manager 6.7 system must have a 64-bit DSN. This requirement applies to all supported databases.

Procedure

1 From the Windows Start menu, select **Control Panel > Administrative Tools > Data Sources (ODBC)**.

2 Create a system DSN.

   If you have a Microsoft SQL database, create the system DSN by using SQL Native Client version 10 or 11.

3 Test the connectivity.

The system now has a DSN that is compatible with Update Manager. When the Update Manager installer prompts you for a DSN, select the 64-bit DSN.

About the Bundled Microsoft SQL Server 2012 Express Database Package

The Microsoft SQL Server 2012 Express database package is installed and configured when you select Microsoft SQL Server 2012 Express as your database during the Update Manager installation or upgrade.

No additional configuration is required.

Maintaining Your Update Manager Database

After your Update Manager database instance and Update Manager server are installed and operational, perform standard database maintenance processes.

Maintaining your Update Manager database involves several tasks:

- Monitoring the growth of the log file and compacting the database log file, as needed. See the documentation for the database type that you are using.
- Scheduling regular backups of the database.
- Backing up the database before any Update Manager upgrade.

See your database documentation for information about backing up your database.

Configure a Microsoft SQL Server Database Connection

When you install Update Manager, you can establish an ODBC connection with a SQL Server database.

If you use SQL Server for Update Manager, do not use the master database.

See your Microsoft SQL ODBC documentation for specific instructions on configuring the SQL Server ODBC connection.

Procedure

1 Create a SQL Server database by using SQL Server Management Studio on SQL Server.

   The Update Manager installer creates all tables, procedures, and user-defined functions (UDF) within the default schema of the database user that you use for Update Manager. This default schema does not necessarily have to be dbo schema.

2 Create a SQL Server database user with database operator (DBO) rights.

   Make sure that the database user has either a **sysadmin** server role or the **db_owner** fixed database role on the Update Manager database and the MSDB database.

   The **db_owner** role on the MSDB database is required for installation and upgrade only.

Create a New Data Source (ODBC)

To prepare a Microsoft SQL Server database to work with Update Manager, you have to create a data source (ODBC).

Procedure

1 On your Update Manager server system, select **Control Panel > Administrative Tools > Data Sources (ODBC)**.

2 Click the **System DSN** tab.

3 Create or modify an ODBC system data source.

Option	Action
Create an ODBC system data source	a Click **Add**. b For Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2 Express, Microsoft SQL Server 2012, or Microsoft SQL Server 2014 select **SQL Native Client**, and click **Finish**.
Modify an existing ODBC system data source	Double-click the ODBC system data source that you want to modify.

To see a detailed list of all Microsoft SQL Server database versions that are compatible with the Update Manager server and the UMDS, select the **Solution/Database Interoperability** option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

4 In the Microsoft SQL Server DSN Configuration window, enter the necessary information and click **Next**.

   a Type an ODBC DSN in the **Name** text field.

      For example, type `VUM`.

   b (Optional) Type an ODBC DSN description in the **Description** text field.

   c Select the SQL Server name from the **Server** drop-down menu.

      Type the SQL Server machine name in the text field if you cannot find it in the drop-down menu.

5 Configure the SQL Server authentication, and click **Next**.

   - If you are using a local SQL Server, you can select **Integrated Windows NT authentication**.
   - If you are using a remote SQL Server, you must use the SQL Server authentication method.

   If you use the SQL Server authentication method, in the **Update Manager installation** wizard supply the same user name, password, and ODBC DSN that you used to configure the ODBC.

   Important Update Manager does not support Windows authentication of the database when the database is located on a different machine because of local system account issues. Make sure that if the Update Manager database is on a remote machine, the database, and the system DSN use SQL Server authentication.

6 Select a database from the **Change the default database to** drop-down menu, specify the ANSI settings, and click **Next**.

7 Specify the language and translation settings, where to save the log files, and click **Finish**.

What to do next

To test the data source, in the **ODBC Microsoft SQL Server Setup** window, click **Test Data Source**, and click **OK**. Ensure that SQL Agent is running on your database server by double-clicking the SQL Server icon in the system tray.

Identify the SQL Server Authentication Type

You can identify whether your SQL Server is using Windows NT or SQL Server authentication.

Procedure

1 Open SQL Server Enterprise Manager.

2 Click the **Properties** tab.

3 Check the connection type.

Configure an Oracle Database

To use an Oracle database for Update Manager, you must first set up the database.

Procedure

1 Download Oracle 11g or Oracle 12c from the Oracle Web site, install it, and create a database (for example, `VUM`).

   Make sure that the TNS Listener is up and running, and test the database service to be sure it is working.

2 Download Oracle ODBC from the Oracle Web site.

3 Install the corresponding Oracle ODBC driver through the Oracle Universal Installer.

4 Increase the number of open cursors for the database.

   Add the entry **`open_cursors = 300`** to the *`ORACLE_BASE`*`\ADMIN\VUM\pfile\init.ora` file.

   In this example, *ORACLE_BASE* is the root of the Oracle directory tree.

Configure an Oracle Connection to Work Locally

You can configure an Oracle connection to work locally with Update Manager.

Prerequisites

Verify that the ODBC data source that you use is a 64-bit system DSN. See Create a 64-Bit DSN.

Procedure

1 Create a tablespace specifically for Update Manager by using the following SQL statement:

```
CREATE TABLESPACE "VUM" DATAFILE 'ORACLE_BASE\ORADATA\VUM\VUM.dat' SIZE 1000M AUTOEXTEND ON NEXT
500K;
```

   In this example, *ORACLE_BASE* is the root of the Oracle directory tree.

2 Create a user, such as vumAdmin, for accessing this tablespace through ODBC.

```
CREATE USER vumAdmin IDENTIFIED BY vumadmin DEFAULT TABLESPACE “vum”;
```

3 Either grant the **dba** permission to the user, or grant the following specific permissions to the user.

```
grant connect to vumAdmin
grant resource to vumAdmin
grant create any job to vumAdmin
grant create view to vumAdmin
grant create any sequence to vumAdmin
grant create any table to vumAdmin
grant lock any table to vumAdmin
grant create procedure to vumAdmin
grant create type to vumAdmin
grant execute on dbms_lock to vumAdmin
grant unlimited tablespace to vumAdmin
# To ensure space limitation is not an issue
```

4 Create an ODBC connection to the database.

See the following example settings:

```
Data Source Name: VUM
TNS Service Name: VUM
User ID: vumAdmin
```

Configure an Oracle Database to Work Remotely

You can configure your Oracle database to work with Update Manager remotely.

Prerequisites

- Verify that the ODBC data source that you use is a 64-bit system DSN. See Create a 64-Bit DSN.
- Set up a database as described in Configure an Oracle Database.

Procedure

1 Install the Oracle client on the Update Manager server machine.

2 Use the Net Configuration Assistant tool to add the entry to connect to the managed host.

```
VUM =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS=(PROTOCOL=TCP)(HOST=host_address)(PORT=1521))
)
(CONNECT_DATA =(SERVICE_NAME = VUM)
)
)
```

In this example, *host_address* is the managed host to which the client needs to connect.

3 (Optional) Edit the `tnsnames.ora` file located in *ORACLE_HOME*`\network\admin\`, as appropriate.

Here, *ORACLE_HOME* is located under `C:\`*ORACLE_BASE*, and it contains subdirectories for Oracle software executable and network files.

4 Create an ODBC connection to the database.

These are example settings.

```
Data Source Name: VUM
TNS Service Name: VUM
User Id: vumAdmin
```

Installing Update Manager on Windows

The Update Manager server is a 64-bit application. You can install the Update Manager server for Windows only on 64-bit Windows machines.

You can install the Update Manager server component either on the same machine where the vCenter Server is installed or on a separate machine. For optimal performance, especially in large-scale environments, install the Update Manager server component on a different Windows machine.

The Update Manager 6.7 installer for Windows generates a 2048-bit key and self-signed certificate. To replace the self-signed SSL certificate after installation, you can use the Update Manager Utility.

You can install vCenter Server and the Update Manager server in a heterogeneous network environment, where one of the machines is configured to use IPv6 and the other is configured to use IPv4.

To run and use Update Manager, you must use a local system account for the machine on which Update Manager is installed.

During installation, you cannot connect an Update Manager server that is installed on a Windows server to a vCenter Server Appliance. The vCenter Server Appliance facilitates Update Manager server as a service.

After you install the Update Manager server component, the Update Manager client interface is automatically enabled on the vSphere Web Client.

In the vSphere Web Client the Update Manager client interface appears as tab **Update Manager**. The **Update Manager** tab is a first level tab and is last in the row of first level tabs, following the **Summary**, the **Monitor**, the **Configure**, the **Permissions**, and so on tabs.

When you use an Update Manager server instance that runs on Windows, you can use Update Manager only with the vSphere Web Client. The vSphere Client does not support using Update Manager server that runs on Windows and is connected to a vCenter Server instance that also runs on Windows. To use Update Manager capabilities with the vSphere Client, use a vCenter Server Appliance where Update Manager runs as a service.

VMware uses designated ports for communication. The Update Manager server connects to vCenter Server, ESXi hosts, and the vSphere Web Client on designated ports. If a firewall exists between any of these elements and Windows firewall service is in use, the installer opens the ports during the installation. For custom firewalls, you must manually open the required ports.

You can run Update Manager in deployments that you protect using SRM. Use caution before connecting the Update Manager server to a vCenter Server instance to which the SRM server is connected. Connecting the Update Manager server to the same vCenter Server instance as SRM might cause problems when you upgrade SRM or vSphere, and when you perform daily tasks. Check the compatibility and interoperability of Update Manager with SRM before you install the Update Manager server.

Prerequisites for Installing the Update Manager Server on Windows

Before you install the Update Manager server, review the installation prerequisites.

Update Manager Database Requirements

Update Manager requires an Oracle or SQL Server database. Update Manager can handle small-scale environments using the bundled Microsoft SQL Server 2012 Express. For environments with more than 5 hosts and 50 virtual machines, you must create either an Oracle or SQL Server database.

To see a list of database formats that are compatible with the Update Manager server and the UMDS, select the **Solution/Database Interoperability** option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

For large-scale environments, set up the database on a machine different than the machines on which the Update Manager server is installed and the vCenter Server database is located. For more information about setting up the Update Manager database, see Preparing the Update Manager Database.

- Create a database and 64-bit DSN, unless you are using the bundled Microsoft SQL Server 2012 Express.
- Make sure that if the Update Manager database is located on a remote machine, the database and the system DSN use SQL Server authentication.

  Update Manager does not support Windows authentication of the database when the database is located on a different machine because of local system account problems.
- If you plan to use the bundled Microsoft SQL Server 2012 Express database, make sure that you install Microsoft Windows Installer version 4.5 (MSI 4.5) on your system.
- Make sure that the database privileges meet the requirements listed in Required Database Privileges.
- Create the 64-bit ODBC connection to a supported database server version by using a supported database client version.

  If you create an ODBC connection to a database server that is of an unsupported version, and your database client is of a supported version, a DSN for the unsupported database might be displayed in the drop-down menu of the Update Manager installation wizard.

vCenter Server Installation

- Install vCenter Server.

If prompted, you must restart the machine on which vCenter Server is installed. Otherwise, you might not be able to register Update Manager with vCenter Server, and the Update Manager installation might fail.

For more information about installing vCenter Server, see *vSphere Installation and Setup*.

- Gather the following networking information for the vCenter Server system.
  - User name and password for the vCenter Server system.

    During the Update Manager installation process, you must register the Update Manager server with the vCenter Server system. To register Update Manager with vCenter Server, you must provide the credentials of the vCenter Server user that has the **Register extension** privilege. For more information about managing users, groups, roles, and permissions, see *vSphere Security*.
  - Port numbers. In most cases, the default Web service port 80 is used.
  - IP address.

    If the IP address of the vCenter Server system or Update Manager changes, you can re-register the Update Manager server with the vCenter Server system. For more information about configuring the Update Manager server after installation, see *Reconfiguring VMware vSphere Update Manager*.

Update Manager System Requirements

- Make sure that your system meets the requirements specified in System Requirements.

Important You can install the Update Manager 6.7 server component only on a 64-bit machine. Make sure the Windows system on which you are installing the Update Manager server is not an Active Directory domain controller.

- Log in as a local Administrator or a domain user that is member of the Administrators group.
- Update Manager installation requires installation of the Microsoft .NET framework 4.7. Consider the following before proceeding with the installation.
  - Installing Microsoft .NET framework 4.7 is not supported on Microsoft Windows Server 2008 Service Pack 2 64-bit.
  - Installing Microsoft .NET framework 4.7 might require you to install some additional Windows updates. Relevant links to the Windows updates are provided during the Microsoft .NET framework 4.7.
  - Installing Microsoft .NET framework 4.7 might require you to reboot your host operating system.
  - If you plan to install Update Manager server on the same Windows machine where vCenter Server runs (typical installation), the vCenter Server service might temporarily disconnect if the a reboot is invoked on the system by the .NET Microsoft .NET framework 4.7 installation.
  - After installing or upgrading the Microsoft .NET framework 4.7, follow the prompts of the Update Manager server or the UMDS installation wizards.

- Check the compatibility and interoperability of the vCenter Server server with VMware Site Recovery Manager®. Use caution when connecting the Update Manager server to a vCenter Server instance to which the Site Recovery Manager server is also connected. Connecting the Update Manager server to the same vCenter Server instance as Site Recovery Manager might cause problems when you upgrade the Site Recovery Manager or the vCenter Server, or when you perform daily operations.

Obtain the Update Manager Installer

You install the Update Manager server for Windows from the vCenter Server installer for Windows.

Update Manager for Windows runs only on a 64-bit Windows operating system.

Prerequisites

Create a My VMware account at https://my.vmware.com/web/vmware/.

Procedure

1 Download the vCenter Server installer from the VMware website at https://my.vmware.com/web/vmware/downloads.

   vCenter Server is part of VMware vCloud Suite and of VMware vSphere, listed under Datacenter & Cloud Infrastructure.

   a Under **Datacenter & Cloud Infrastructure**, select **VMware vCloud Suite or VMware vSphere**, and click **Download Product**.

   b From the **Select Version** drop-down menu, select the version you want.

   c Locate VMware vCenter Server on the page, and select **Go to Downloads**.

   d Download the ISO file of the VMware vCenter Server *<product version>* and Modules for Windows.

2 Confirm that the md5sum is correct.

   See the VMware website topic Using MD5 Checksums at http://www.vmware.com/download/md5.html.

3 Mount the ISO image to the Windows virtual machine or physical server on which you want to install the Update Manager server or the UMDS.

Install the Update Manager Server

The Update Manager installation requires a connection with a single vCenter Server instance. You can install Update Manager on the same computer on which vCenter Server is installed or on a different computer.

When you use an Update Manager server instance that runs on Windows, you can use Update Manager only with the vSphere Web Client. The vSphere Client does not support using Update Manager server that runs on Windows and is connected to a vCenter Server instance that also runs on Windows. To use Update Manager capabilities with the vSphere Client, use a vCenter Server Appliance where Update Manager runs as a service.

Prerequisites

- See installation prerequisites in Prerequisites for Installing the Update Manager Server on Windows.
- Check the compatibility and interoperability of the vCenter Server server with VMware Site Recovery Manager®. Use caution when connecting the Update Manager server to a vCenter Server instance to which the Site Recovery Manager server is also connected. Connecting the Update Manager server to the same vCenter Server instance as Site Recovery Manager might cause problems when you upgrade the Site Recovery Manager or the vCenter Server, or when you perform daily operations.
- Update Manager installation requires installation of the Microsoft .NET framework 4.7. Consider the following before proceeding with the installation.
  - Installing Microsoft .NET framework 4.7 is not supported on Microsoft Windows Server 2008 Service Pack 2 64-bit.
  - Installing Microsoft .NET framework 4.7 might require you to install some additional Windows updates. Relevant links to the Windows updates are provided during the Microsoft .NET framework 4.7.
  - Installing Microsoft .NET framework 4.7 might require you to reboot your host operating system.
  - If you plan to install Update Manager server on the same Windows machine where vCenter Server runs (typical installation), the vCenter Server service might temporarily disconnect if the a reboot is invoked on the system by the .NET Microsoft .NET framework 4.7 installation.
  - After installing or upgrading the Microsoft .NET framework 4.7, follow the prompts of the Update Manager server or the UMDS installation wizards.

Procedure

1. Mount the ISO image of the vCenter Server installer to the Windows virtual machine or physical server on which you want to install the Update Manager server.
2. In the mounted directory, double-click the `autorun.exe` file of the VMware vCenter Installer, and select **vSphere Update Manager > Server**.
3. (Optional) Select the option to **Use Microsoft SQL Server 2012 Express as the embedded database**, and click **Install**.

   Note Skip this step only if you plan to use another supported Oracle or SQL Server database.

   If the Microsoft SQL Server 2012 Express is not present on your system from previous Update Manager installations, the installation wizard for the Microsoft SQL Server 2012 Express opens.
4. Select the option to install the Microsoft .NET framework 4.7.

   Note If you do not select to install Microsoft .NET framework 4.7, the Update Manager server installation will fail with an error message.

5 On the **VMware vCenter Installer**, click **Install**.

The **VMware vCenter Installer** wizard remains open, and a language selection dialog box opens.

6 Select the language for the vSphere Update Manager installer, and click **OK**.

7 Depending on the database selection you made in the VMware vCenter Installer, perform one of the following steps:

- If you selected to use embedded Microsoft SQL Server 2012, wait for the installation process of the Microsoft .NET framework 4.7 and the Microsoft SQL Server 2012 to complete, and from the VMware vCenter Installer, click **Install** again.

  The VMware vSphere Update Manager installer opens.

- If you are using another supported database and did not select to use the embedded Microsoft SQL Server 2012, the VMware vSphere Update Manager installer opens, and you can proceed with next steps.

8 Review the Welcome page and click **Next**.

9 Read and accept the license agreement, and click **Next**.

10 Review the support information, select whether to download updates from the default download sources immediately after installation, and click **Next**.

If you deselect **Download updates from default sources immediately after installation**, Update Manager downloads updates once daily according to the default download schedule or immediately after you click the **Download Now** button on the Download Settings page. You can modify the default download schedule after the installation is complete.

11 Type the vCenter Server IP address or name, HTTP port, and the administrative account that the Update Manager server will use to connect to the vCenter Server system, and click **Next**.

You can not provide an IP address to a vCenter Server Appliance. Update Manager server is fully integrated with the vCenter Server Appliance, and the vCenter Server Appliance runs Update Manager as a service.

The default administrative user account is administrator@vsphere.local.

12 (Optional) Select the database, and click **Next**.

If you selected to use the embedded Microsoft SQL Server 2012 Express database, the installation wizard skips this page.

a Use an existing supported database, by selecting your database from the list of DSNs. If the DSN does not use Windows NT authentication, enter the user name and password for the DSN and click **Next**.

Important The DSN must be a 64-bit DSN.

13 (Optional) Select the database options.

- If the system DSN you specify points to an existing Update Manager database with the current schema, you can either retain your existing database or replace it with an empty one.
- If the system DSN you specify points to an existing Update Manager database with a different schema, on the Database Upgrade page, select **Yes, I want to upgrade my Update Manager database** and **I have taken a backup of the existing Update Manager database**, and click **Next**.

14 From the drop-down menu, select the IP address or the host name of your Update Manager instance.

If the computer on which you install Update Manager has one NIC, the Update Manager installer automatically detects the IP address. If the computer has multiple NICs, you must select the correct IP address or use a DNS name. The DNS name must be resolved from all hosts that this Update Manager instance will manage.

15 Specify the Update Manager port settings, select whether you want to configure the proxy settings, and click **Next**.

Note Use caution when you specify the Update Manager port settings, as you cannot modify them after installation.

For the SOAP port, you have no limitations to the range of ports used, unless there are conflicts.

For the Server port, you can use the following range: 80, 9000-9100. Update Manager automatically opens ESXi firewall ports in this range to allow outbound HTTP traffic to the patch store.

16 (Optional) Provide information about the proxy server, the port, and whether the proxy should be authenticated, and click **Next**.

17 Select the Update Manager installation and patch download directories, and click **Next**.

If you do not want to use the default locations, you can click **Change** to browse to a different directory.

18 (Optional) In the warning message about the disk free space, click **OK**.

This message appears when you try to install Update Manager on a computer that has less than 120 GB free space.

19 Click **Install** to begin the Update Manager server installation.

20 Click **Finish** to close the Update Manager installation wizard.

The Update Manager server component is installed. The Update Manager client interface is automatically enabled in the vSphere Web Client.

Note When you use an Update Manager server instance that runs on Windows, you can use Update Manager only with the vSphere Web Client. If you use the vSphere Client to connect to the vCenter Server instance to which the Update Manager server that runs on Windows is registered, you do not see any Update Manager interface.

Using the Update Manager Client Interface with Update Manager Server that Runs on Windows

The Update Manager client interface do not require any installation, and is automatically enabled in the vSphere Web Client after you install the Update Manager server component on Windows.

When you use an Update Manager server instance that runs on Windows, you can use Update Manager only with the vSphere Web Client. The vSphere Client does not support using Update Manager server that runs on Windows and is connected to a vCenter Server instance that also runs on Windows. To use Update Manager capabilities with the vSphere Client, use a vCenter Server Appliance where Update Manager runs as a service.

With the Update Manager client interface in the vSphere Web Client, you can perform the full set of operations that Update Manager offers. You can create and manage baselines, attach and detach baselines to hosts and VMs, scan for compliance, perform upgrade operations on the hosts and update operations the virtual machines in your environment, manage the Update Manager configuration settings.

Verify that you have the **View Compliance Status** privilege, otherwise you cannot see and use the Update Manager client interface in the vSphere Web Client.

In the vSphere Web Client the Update Manager client interface appears as tab **Update Manager**. The **Update Manager** tab is a first level tab and is last in the row of first level tabs, following the **Summary**, the **Monitor**, the **Configure**, the **Permissions**, and so on tabs.

For more information, see Overview of the Update Manager Client Interfaces.

Upgrading Update Manager that Runs on Windows

You can upgrade to Update Manager 6.7 only from Update Manager versions 6.0 or 6.5 that are installed on a 64-bit Windows operating system.

If you are switching from using a vCenter Server system of version 6.0 or version 6.5 that runs on Windows to a vCenter Server Appliance 6.7, this is a migration process. For detailed information on Update Manager migration process, read Chapter 4 Migrating Update Manager from Windows to the vCenter Server Appliance, or see the Migration chapter in *vSphere Upgrade* documentation.

If you are running Update Manager of a version earlier than 5.5, or Update Manager that runs on a 32-bit platform, you cannot perform a direct upgrade to Update Manager 6.7. You must use the data migration tool that is provided with Update Manager 5.0 installation media to upgrade your Update Manager system to Update Manager 5.0 running on a 64-bit operating system, and then perform an upgrade from version 5.0 or version 5.1 to version 5.5 before upgrading to version 6.7. For detailed information how to use the data migration tool, see the *Installing and Administering VMware vSphere Update Manager* documentation for Update Manager 5.0.

When you upgrade Update Manager, you cannot change the installation path and patch download location. To change these parameters, you must install a new version of Update Manager rather than upgrade.

Previous versions of Update Manager use a 512-bit key and self-signed certificate and these are not replaced during upgrade. If you require a more secure 2048-bit key, you can either perform a new installation of Update Manager 6.7, or use the Update Manager Utility to replace the existing certificate. For more information about how to use the Update Manager Utility, see the *Reconfiguring VMware vSphere Update Manager* documentation.

Scheduled tasks for virtual machine patch scan and remediation are retained during the upgrade. After the upgrade, you can edit and remove scheduled scan tasks that exist from previous releases. You can remove existing scheduled remediation tasks but you cannot edit them.

You must upgrade the Update Manager database during the Update Manager upgrade. You can select whether to keep your existing data in the database or to replace it during the upgrade.

The Java Components (JRE) required by Update Manager are installed or upgraded silently on the system when you install or upgrade Update Manager. You can upgrade the Java Components separately from an Update Manager upgrade procedure to a version of the Java Components that is released asynchronously from the Update Manager releases.

Upgrade the Update Manager Server

To upgrade an instance of Update Manager that is installed on a 64-bit machine, you must first upgrade vCenter Server to a compatible version.

The Update Manager 6.7 release allows upgrades from Update Manager 6.0 or later.

Prerequisites

- Grant the database user the required set of privileges. For more information, see Preparing the Update Manager Database.
- Stop the Update Manager service and back up the Update Manager database. The installer upgrades the database schema, making the database irreversibly incompatible with previous Update Manager versions.
- If you are upgrading Update Manager instance that uses Oracle database, Create a 64-Bit DSN. If you are upgrading Update Manager instance that uses Microsoft SQL database, the creation of 64-bit DSN is managed by the installer.
- See information about Update Manager Compatibility with vCenter Server, vCenter Server Appliance, vSphere Web Client, and vSphere Client.

Procedure

1 Upgrade vCenter Server to a compatible version.

   Note The vCenter Server installation wizard warns you that Update Manager is not compatible when vCenter Server is upgraded.

   If prompted, you must restart the machine that is running vCenter Server. Otherwise, you might not be able to upgrade Update Manager.

2 In the software installer directory, double-click the `autorun.exe` file and select **vSphere Update Manager > Server**.

   If you cannot run `autorun.exe`, browse to the `UpdateManager` folder and run `VMware-UpdateManager.exe`.

3 Select a language for the installer and click **OK**.

4 In the upgrade warning message, click **OK**.

5 Review the Welcome page and click **Next**.

6 Read and accept the license agreement, and click **Next**.

7 Review the support information, select whether to download updates from the default download sources immediately after installation, and click **Next**.

   If you deselect **Download updates from default sources immediately after installation**, Update Manager downloads updates once daily according to the default download schedule or immediately after you click **Download Now** on the Download Settings page. You can modify the default download schedule after the installation is complete.

8 Type the vCenter Server system credentials and click **Next**.

   To keep the Update Manager registration with the original vCenter Server system valid, keep the vCenter Server system IP address and enter the credentials from the original installation.

9 Type the database password for the Update Manager database and click **Next**.

   The database password is required only if the DSN does not use Windows NT authentication.

10 On the Database Upgrade page, select **Yes, I want to upgrade my Update Manager database** and **I have taken a backup of the existing Update Manager database**, and click **Next**.

11 (Optional) On the Database re-initialization warning page, select to keep your existing remote database if it is already upgraded to the latest schema.

   If you replace your existing database with an empty one, you lose all of your existing data.

12 Specify the Update Manager port settings, select whether you want to configure the proxy settings, and click **Next**.

   Configure the proxy settings if the computer on which Update Manager is installed has access to the Internet.

13 (Optional) Provide information about the proxy server and port, specify whether the proxy should be authenticated, and click **Next**.

14 Click **Install** to begin the upgrade.

15 Click **Finish**.

You upgraded the Update Manager server.

Upgrade the Update Manager Java Components

The required Update Manager Java Components (JRE) are installed or upgraded silently when you install or upgrade Update Manager. By using a vCenter Server Java components patch, you can also upgrade Update Manager Java Components separately from Update Manager installer.

By using the separate installer, you can upgrade JRE to a version that is released asynchronously from Update Manager releases. If an earlier version of JRE is present on the system, this procedure upgrades it.

When Update Manager runs on the same system as the vCenter Server, if an earlier version of vCenter Server tc Server is present on that system, this procedure also upgrades the vCenter Server tc Server component.

During the patch process, the Update Manager undergoes a downtime as the vCenter Server Java Components patch restarts the Update Manager service.

Prerequisites

- Download the vCenter Server Java Components patch from VMware downloads page at https://my.vmware.com/web/vmware/downloads. The name format is `VMware-VIMPatch-6.7.0-`*`build_number-YYYYMMDD`*`.iso`.
- Stop any running Update Manager operations, such as scanning, staging, or remediation.

Procedure

1. On the system where Update Manager is installed, mount the ISO of the vCenter Server Java Components patch.
2. In Windows Explorer, double-click the file *`ISO_mount_directory`*`/autorun.exe`.

   A **vCenter Server Java Components Update** wizard opens.
3. Click **Patch All**.

   If the Java components on the Update Manager system are up to date, a status message that confirms that is displayed.

   If the Java components on the Update Manager system are not up to date, they are silently upgraded.

   When clicking the **Patch All** button, if vCenter Server, vCenter Single Sign-On, vCenter Inventory Service, or vSphere Web Client are also installed on the system where Update Manager is installed, the Java components for all thesevCenter Server components are also silently upgraded.

The Java components are upgraded on the Update Manager system.

Uninstalling Update Manager that Runs on Windows

Update Manager has a relatively small impact on computing resources such as disk space. Unless you are certain that you want to remove Update Manager, leave an existing installation in place.

When you uninstall the Update Manager server, the Update Manager client interface is automatically removed from the vSphere Web Client.

Uninstall the Update Manager Server that Runs on Windows

You can uninstall the Update Manager server component.

Procedure

1 From the Windows **Start** menu, select **Settings > Control Panel > Add or Remove Programs**.

2 Select **VMware vSphere Update Manager** and click **Remove**.

The Update Manager server component is uninstalled from your system. All downloaded metadata and binaries, as well as log data remain on the machine where Update Manager server was installed.

The Update Manager client interface is automatically removed from the vSphere Web Client.

Best Practices and Recommendations for Update Manager Environment

You can install Update Manager on the server on which vCenter Server runs or on a different server.

The Update Manager server and client plug-ins must be the same version. Update Manager and vCenter Server, and the vSphere Web Client must be of a compatible version. For more information about compatibility, see Update Manager Compatibility with vCenter Server, vCenter Server Appliance, vSphere Web Client, and vSphere Client.

Update Managerr has two deployment models:

Internet-connected model The Update Manager server is connected to the VMware patch repository, and third-party patch repositories (for ESXi 6.x hosts). Update Manager works with vCenter Server to scan and remediate the virtual machines, hosts, and templates.

Air-gap model Update Manager has no connection to the Internet and cannot download patch metadata. In this model, you can use UMDS to download and store patch metadata and patch binaries in a shared repository. To scan and remediate inventory objects, you must configure the Update Manager server to use a shared repository of UMDS data as a patch datastore. For more information about using UMDS, see Chapter 6 Installing, Setting Up, and Using Update Manager Download Service.

Outside of DRS clusters, you might not be able to remediate the host running the Update Manager or vCenter Server virtual machines by using the same vCenter Server instance, because the virtual machines cannot be suspended or shut down during remediation. You can remediate such a host by using separate vCenter Server and Update Manager instances on another host. Inside DRS clusters, if you start a remediation task on the host running the vCenter Server or Update Manager virtual machines, DRS attempts to migrate the virtual machines to another host, so that the remediation succeeds. If DRS cannot migrate the virtual machine running Update Manager or vCenter Server, the remediation fails. Remediation also fails if you have selected the option to power off or suspend the virtual machines before remediation.

Update Manager Deployment Models on Windows and Their Usage

You can use the different Update Manager deployment models in different cases, depending on the size of your system.

You can use one of several common host-deployment models for Update Manager server:

All-in-one model

vCenter Server and Update Manager server are installed on one host and their database instances are on the same host. This model is most reliable when your system is relatively small.

Medium deployment model

vCenter Server and Update Manager server are installed on one host and their database instances are on two separate hosts. This model is recommended for medium deployments, with more than 300 virtual machines or 30 hosts.

Large deployment model

vCenter Server and Update Manager server run on different hosts, each with its dedicated database server. This model is recommended for large deployments when the datacenters contain more than 1,000 virtual machines or 100 hosts.

Update Manager in the vCenter Server Appliance 3

You can use the Update Manager 6.7 as a service of the vCenter Server Appliance 6.7. The Update Manager server and client components are part of the vCenter Server Appliance.

When you deploy the vCenter Server Appliance, the VMware vSphere Update Manager Extension service starts automatically.

Attempts to connect Update Manager server during installation on a Windows operating system to a vCenter Server Appliance fail with an error. Beginning with vSphere 6.5 an later releases, registering a Update Manager server instance that runs on Windows to a vCenter Server Appliance is not supported.

The Update Manager extension for the vCenter Server Appliance uses a PostgreSQL database that is bundled with the Appliance. Although the Update Manager and the vCenter Server Appliance share the same PostgreSQL database server, they have separate database instances. If you must reset the Update Manager database, the vCenter Server Appliance database remains intact.

After deploying the vCenter Server Appliance, the Update Manager user interfaces are automatically enabled in both the vSphere Client and the vSphere Web Client. However, there are some differences in the available Update Manager functionality in the two vSphere clients. For more information, see Overview of the Update Manager Client Interfaces.

Unlike the Update Manager instance that runs on Windows, with the Update Manager instance that runs in the vCenter Server Appliance you can make certain configurations changes directly from the vSphere Web Client. You can change the values for Download patches on service start, Log Level, SOAP Port, Web Server Port, and Web SSL Port. You can access these settings from **System Configuration > Services**, under vSphere Web Client Administration. After you change these settings, restart the VMware vSphere Update Manager service for the changes to take effect.

For Update Manager that runs in the vCenter Server Appliance the only configuration you cannot change from the vSphere Web Client is the certificate that Update Manager uses to authenticate to vCenter Server. You can change the certificate by using the Update Manager Utility.

The Update Manager Utility is also bundled with the vCenter Server Appliance. You can access the Update Manager Utility from the Bash Shell of the vCenter Server Appliance.

This chapter includes the following topics:

- System Requirements for the vCenter Server Appliance and Update Manager
- Using the Update Manager Client Interfaces with Update Manager Service that Runs in the vCenter Server Appliance

- Start, Stop, or Restart Update Manager Service in the vCenter Server Appliance

System Requirements for the vCenter Server Appliance and Update Manager

When you deploy a vCenter Server Appliance 6.5 or later, Update Manager automatically starts running as a service in the appliance.

The number of hosts and VMs that you can upgrade with Update Manager in the vCenter Server Appliance depends on the size of the vSphere environment that the vCenter Server Appliance is suitable for.

For information about the vSphere environment size and corresponding system requirements for the vCenter Server Appliance, see the *vCenter Server Installation and Setup* documentation here.

Using the Update Manager Client Interfaces with Update Manager Service that Runs in the vCenter Server Appliance

The Update Manager client interface do not require any installation, and is automatically enabled in both the vSphere Web Client and the vSphere Client after you deploy the vCenter Server Appliance.

With the Update Manager client interface in the vSphere Web Client, you can perform the full set of operations that Update Manager offers. You can create and manage baselines, attach and detach baselines to hosts and VMs, scan for compliance, perform upgrade operations on the hosts and update operations the virtual machines in your environment, manage the Update Manager configuration settings.

With the Update Manager client interface for the vSphere Client, you can perform a limited set of Update Manager operations. You can create, attach and detach baselines, monitor host and cluster compliance, remediate hosts and clusters. With vSphere Client 6.7 you cannot change Update Manager configuration settings, remediate VMs, or change the default options for the remediation process in the remediation wizard. For any of the limited functionality, you must use the vSphere Web Client.

For more information, see Overview of the Update Manager Client Interfaces.

Start, Stop, or Restart Update Manager Service in the vCenter Server Appliance

If you make configuration changes to Update Manager settings, you might need restart the Update Manager service in the vCenter Server Appliance.

Note Starting with vSphere 6.5, all vCenter Server services and some Platform Services Controller services run as child processes of the VMware Service Lifecycle Manager service.

Prerequisites

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

Procedure

1 Log in to the vCenter Server by using the vSphere Web Client.

2 On the vSphere Web Client Home page, click **System Configuration**.

3 Under System Configuration, click **Services**.

4 From the Services list, select the VMware vSphere Update Manager service.

5 From the **Actions** menu, select an operation name.

   - **Restart**
   - **Start**
   - **Stop**

Migrating Update Manager from Windows to the vCenter Server Appliance

4

For vSphere 6.0 and earlier releases, 64-bit Windows operating systems are the only supported host operating systems for Update Manager. In vSphere 6.5, Update Manager is provided as an optional service in the vCenter Server Appliance 6.5. VMware provides supported paths for migrating Update Manager from a Windows operating system to a vCenter Server Appliance 6.5.

You can migrate Update Manager in the following vCenter Server deployments:

Table 4-1. Supported Migration Paths for Update Manager That Runs on Windows to a vCenter Server Appliance

Source Configuration	Target Configuration
vCenter Server and Update Manager run on the same Windows machine	vCenter Server Appliance 6.7 with embedded Update Manager
vCenter Server and Update Manager run on different Windows machines	vCenter Server Appliance 6.7 with embedded Update Manager
Update Manager run on a Windows machine and is connected to a vCenter Server Appliance	vCenter Server Appliance 6.7 with embedded Update Manager

You can use a GUI method or a CLI method to upgrade or migrate your vCenter Server deployment that uses external Update Manager instance. If you use the GUI method, you need to perform manual steps on the Update Manager Windows system. If you use the CLI method, you need to add configuration parameters about Update Manager in your JSON template.

For detailed information about the GUI method or the CLI upgrade or migration configuration parameters, see the *vSphere Upgrade* documentation.

Important Verify that the Update Manager source machine does not run additional extensions that are connected to other vCenter Server systems, which are not part of your migration.

Before the migration, Update Manager might use any of the supported Microsoft SQL Server, or Oracle, or the Embedded database solution. After the migration to the vCenter Server Appliance, Update Manager starts to use the PostgreSQL Database.

After the migration, you can shut down the Update Manager machine. You might need to keep the Update Manager machine for roll back purposes to the earlier version before the migration.

This chapter includes the following topics:

- Download and Run VMware Migration Assistant on the Source Update Manager Machine
- Roll Back a Migration of vCenter Server Appliance with Update Manager

Download and Run VMware Migration Assistant on the Source Update Manager Machine

Before running a migration from vCenter Server that runs on Windows, or upgrading vCenter Server Appliance that use an external Update Manager, you must download and run the VMware Migration Assistant on the source Windows physical server or the Windows virtual machine where Update Manager runs. The VMware Migration Assistant facilitates the migration of the Update Manager server and database to the vCenter Server Appliance 6.5.

Alternatively, if you plan to perform the CLI method for upgrading your vCenter Server Appliance or migrating your vCenter Server that runs on Windows, you can skip this procedure, and add the `source.vum section section` and `run.migration.assistant subsection` to your JSON template. For information about the CLI upgrade or migration configuration parameters, see the *vSphere Upgrade* documentation.

Caution It is important to run the VMware Migration Assistant on the source Update Manager machine before migrating other of the vCenter Server components.

Prerequisites

- Download the vCenter Server Appliance Installer. For more information, see the *vCenter Server Installation and Setup* documentation.
- Log in to the source Update Manager machine as an administrator.

Procedure

1. From the vCenter Server Appliance installer package, copy the `migration-assistant` folder to the source Update Manager machine.
2. From the `migration-assistant` directory, double-click `VMware-Migration-Assistant.exe`, and provide the vCenter Single Sign-On administrator password.

   Note Leave the Migration Assistant window open during the migration process. Closing the Migration Assistant causes the migration process to stop.

   The VMware Migration Assistant runs pre-upgrade checks and prompts you to resolve any errors it finds before starting the upgrade.

When the pre-checks are finished and any errors are addressed, your source Update Manager system is ready for the migration to the vCenter Server Appliance.

What to do next

Use VMware Migration Assistant to migrate vCenter Server and all its components to vCenter Server Appliance 6.5.

Roll Back a Migration of vCenter Server Appliance with Update Manager

You can roll back a vCenter Server Appliance with Update Manager after a migration.

Rolling back to the vCenter Server version before the upgrade or migration requires to shut down the new appliance and revert to the source appliance or vCenter Server on Windows.

Prerequisites

- You must have access to the source vCenter Server Appliance.
- You must have access to the Update Manager source machine on Windows.

Procedure

1. Power off the newly upgraded or migrated vCenter Server Appliance.
2. Power on the vCenter Server Appliance that Update Manager was connected to before the migration.
3. Start the Windows source machine where Update Manager ran before the migration, and rejoin it to the Active Directory domain.
   - If the source machine was attached to an Active Directory domain and migration failed before network migration, you do not need to perform any additional steps.
   - If the source machine was attached to an Active Directory domain and the migration failed after network migration, log in with the local administrator after the machine powers up and rejoin the machine to the Active Directory domain.

Configuring Update Manager

5

Update Manager runs with the default configuration properties unless you have modified them during the installation. After installation, you might need to change some Update Manager settings. Modifying Update Manager settings is possible only from the Update Manager Admin view that is available in the vSphere Web Client. You cannot manage Update Manager settings from the vSphere Client.

You can configure and modify the Update Manager settings only if you have the privileges to configure the Update Manager settings and service. These permissions must be assigned on the vCenter Server system with which Update Manager is registered. For more information about managing users, groups, roles, and permissions, see *vSphere Security* documentation. For a list of Update Manager privileges and their descriptions, see Update Manager Privileges.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, and multiple vCenter Server instances use Update Manager, you can configure the settings for each Update Manager instance. Configuration properties you modify are applied only to the Update Manager instance you specify, and are not propagated to the other instances in the domain.

To change a certain Update Manager setting, in the vSphere Web Client go to **Home > Update Manager**, and from the list of object select the name of the vCenter Server system with which the Update Manager server is registered. Update Manager settings are available under the **Manage** tab.

This chapter includes the following topics:

- Update Manager Privileges

Update Manager Network Connectivity Settings

The port, IP, and DNS settings are configured during the installation of Update Manager and do not depend on your deployment model.

Default Network Ports

The network port settings are configured during installation but you can change them later to avoid conflicts with other programs installed on the same machine.

Table 5-1. Update Manager Default Network Ports

TCP Port Number	Description
80	The port used by Update Manager to connect to vCenter Server.
9084	The port used by ESXi hosts to access host patch downloads over HTTP.
902	The port used by Update Manager to push host upgrade files.
8084	The port used by Update Manager Client plug-in to connect to the Update Manager SOAP server.
9087	The HTTPS port used by Update Manager Client plug-in to upload host upgrade files.

IP Address and DNS Name

The Update Manager network settings include the IP address or DNS name that the update utility on hosts uses to retrieve the patch metadata and binaries from the Update Manager server (through HTTP). The IP address is configured during installation, but you can change it later from the **IP address or host name for the patch store** drop-down menu on the Network Connectivity page of the **Manage** tab of Update Manager Admin view in the vSphere Web Client.

Important To avoid any potential DNS resolution problems, use an IP address whenever possible. If you must use a DNS name instead of an IP address, ensure that the DNS name you specify can be resolved from all hosts managed by Update Manager as well as by vCenter Server.

Update Manager supports Internet Protocol version 6 (IPv6) environments for scanning and remediating hosts running ESXi 6.0 and later. Update Manager does not support IPv6 for scanning and remediation of virtual machines.

vCenter Server, Update Manager, and your ESXi hosts might exist in a heterogeneous IPv6 and IPv4 network environment. In such an environment, if you use IP addresses, and no dual stack IPv4 or IPv6 DNS servers exist, the ESXi hosts configured to use only IPv4 address cannot access the IPv6 network resources. The hosts configured to use only IPv6 cannot access the IPv4 network resources either.

You can install Update Manager on a machine on which both IPv4 and IPv6 are enabled. During host operations such as scanning, staging, and remediation, Update Manager provides the address of its patch store location to the ESXi hosts. If Update Manager is configured to use an IP address, it provides an IP address of either IPv4 or IPv6 type, and can be accessed only by some of the hosts. For example, if Update Manager provides an IPv4 address, the hosts that use only an IPv6 address cannot access the Update Manager patch store. In such a case, consider the following configuration.

Table 5-2. Update Manager Configuration

Host IP Version	Action
IPv4	Configure Update Manager to use either an IPv4 address or a host name. Using a host name lets all hosts rely on the DNS server to resolve to an IPv4 address.
IPv6	Configure Update Manager to use either an IPv6 address or a host name. Using a host name lets hosts rely on the DNS server to resolve to an IPv6 address.
IPv4 and IPv6	Configure Update Manager to use either IPv4 or IPv6.

Change the Update Manager Network Settings

The network ports are configured during installation. After installation, you can only edit whether to use IP address or host name for the Update Manager patch store.

Prerequisites

- If any remediation or scan tasks are running, cancel them or wait until they complete.
- To obtain metadata for the patches, Update Manager must have access to https://www.vmware.com, and requires outbound ports 80 and 443.

Procedure

1. In the Home view of the vSphere Web Client, select the Update Manager icon.
2. From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
3. Click the **Manage** tab.
4. Click **Settings**, and select **Network Connectivity**.

5 See information about the network connectivity settings for Update Manager.

Option	Description
SOAP port	Update Manager client uses this port to communicate with the Update Manager server.
Server port (range: 80, 9000–9100)	Listening port for the Web server that provides access to the patch depot for ESXi hosts.
IP address or host name for the patch store	The IP address or name of the host where patches are downloaded and stored.

Note You can only edit the IP address or host name for the patch store. The ports are defined during installation.

If you are using Update Manager that runs in the vCenter Server Appliance, you can change the ports from the vCenter Server system configuration. For more information, see Edit the Settings of Services from the vCenter Server and Host Management documentation.

6 Click **Edit**, and select an IP address or host name for the patch store.

Important Use an IP address whenever possible to avoid any potential DNS resolution problems. If you must use a DNS name instead of an IP address, ensure that the DNS name you specify can be resolved from vCenter Server, and the hosts that are managed by Update Manager.

7 Click **OK**.

What to do next

Restart the Update Manager service for network changes to take effect.

Configuring the Update Manager Download Sources

You can configure the Update Manager server to download patches and extensions for ESXi hosts either from the Internet or from a shared repository of UMDS data. You can also import patches and extensions for ESXi hosts manually from a ZIP file.

If your deployment system is connected to the Internet, you can use the default settings and links for downloading upgrades, patches, and extensions to the Update Manager repository. You can also add URL addresses to download third-party patches and extensions. Third-party patches and extensions are applicable only to hosts that are running ESXi 6.0 and later.

Downloading host patches from the VMware Web site is a secure process.

- Patches are cryptographically signed with the VMware private keys. Before you try to install a patch on a host, the host verifies the signature. This signature enforces the end-to-end protection of the patch itself, and can also address any concerns about patch download.

- Update Manager downloads patch metadata and patch binaries over SSL connections.
  Update Manager downloads patch metadata and patch binaries only after verification of both the validity of the SSL certificates and the common name in the certificates. The common name in the certificates must match the names of the servers from which Update Manager downloads patches.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the upgrades, patches, and extensions by using Update Manager Download Service (UMDS).

For more information about UMDS, see Chapter 6 Installing, Setting Up, and Using Update Manager Download Service.

Changing the download source from a shared repository to Internet, and the reverse, is a change in the Update Manager configuration. Both options are mutually exclusive. You cannot download updates from the Internet and a shared repository at the same time. To download new data, you must run the VMware vSphere Update Manager Download task. You can start the task by clicking the **Download Now** button at the bottom of the Download Sources pane.

If the VMware vSphere Update Manager Update Download task is running when you apply the new configuration settings, the task continues to use the old settings until it completes. The next time the task to download updates starts, it uses the new settings.

With Update Manager, you can import both VMware and third-party patches or extensions manually from a ZIP file, also called an offline bundle. Import of offline bundles is supported only for hosts that are running ESXi 6.0 and later. You download the offline bundle ZIP files from the Internet or copy them from a media drive, and save them on a local or a shared network drive. You can import the patches or extensions to the Update Manager patch repository later. You can download offline bundles from the VMware Web site or from the Web sites of third-party vendors.

Note You can use offline bundles for host patching operations only. You cannot use third-party offline bundles or offline bundles that you generated from custom VIB sets for host upgrade from ESXi 6.0 and ESXi 6.5 to ESXi 6.7.

Offline bundles contain one `metadata.zip` file, one or more VIB files, and optionally two `.xml` files, `index.xml` and `vendor-index.xml`.

When you import an offline bundle to the Update Manager patch repository, Update Manager extracts it and checks whether the `metadata.zip` file has already been imported. If the `metadata.zip` file has never been imported, Update Manager performs sanity testing, and imports the files successfully. After you confirm the import, Update Manager saves the files into the Update Manager database and copies the `metadata.zip` file, the VIBs, and the `.xml` files, if available, into the Update Manager patch repository.

- Configure Update Manager to Use the Internet as a Download Source

  If your deployment system is connected to the Internet, you can directly download ESXi patches and extensions.

- Add a New Download Source

  If you use the Internet as a download source for updates, you can add a third-party URL address to download patches and extensions for hosts that are running ESXi 6.0 and later.

- Use a Shared Repository as a Download Source

  You can configure Update Manager to use a shared repository as a source for downloading ESXi patches, extensions, and notifications.

- Import Patches Manually

  Instead of using a shared repository or the Internet as a download source for patches and extensions, you can import patches and extensions manually by using an offline bundle.

Configure Update Manager to Use the Internet as a Download Source

If your deployment system is connected to the Internet, you can directly download ESXi patches and extensions.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1. In the Home view of the vSphere Web Client, select the Update Manager icon.
2. From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
3. Click the **Manage** tab.
4. Click **Settings**, and select **Download Setings**.
5. In the Download Sources pane, click **Edit**.

   An Edit Download Sources dialog box opens.
6. Select the option **Use direct connection to Internet**.
7. Select a download source from the list, and click **Enable** or **Disable** depending on whether you want to download updates from that source.

   You can choose to download host patches and extensions. You cannot edit the download source location of the default ESXi patches and extensions. You can only enable or disable downloading.
8. (Optional) Add an extra third-party download source for hosts that are running ESXi 6.0 and later.
9. Click **OK** to close the Edit Download Sources dialog box.

10 In the Download Sources pane, click **Download Now** to run the Download patch definitions task.

All notifications and updates are downloaded immediately even if the **Enable scheduled download** check box is selected in **Manage > Notification Check Schedule** or **Manage > Download Schedule**, respectively.

Add a New Download Source

If you use the Internet as a download source for updates, you can add a third-party URL address to download patches and extensions for hosts that are running ESXi 6.0 and later.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Download Setings**.

5 In the Download Sources pane, click **Edit**.

An Edit Download Sources dialog box opens.

6 Select the option **Use direct connection to Internet**.

7 Click **Add**.

An Add Download Source dialog box opens.

8 Enter a URL to a new download source.

Update Manager supports both HTTP and HTTPS URL addresses. Use HTTPS URL addresses, so that the data is downloaded securely. The URL addresses that you add must be complete and contain the `index.xml` file, which lists the vendor and the vendor index.

Note The proxy settings for Update Manager are applicable to third-party URL addresses too. You can configure the proxy settings from the Proxy Settings pane.

9 Type a short description for the URL, and click **OK**.

The vSphere Web Client performs validation of the URL.

10 Click **OK** to close the Edit Download Sources dialog box.

11 In the Download Sources pane, click **Download Now** to run the Download patch definitions task.

   All notifications and updates are downloaded immediately even if the **Enable scheduled download** check box is selected in **Manage > Notification Check Schedule** or **Manage > Download Schedule**, respectively.

The location is added to the list of Internet download sources.

Use a Shared Repository as a Download Source

You can configure Update Manager to use a shared repository as a source for downloading ESXi patches, extensions, and notifications.

Prerequisites

- Create a shared repository using UMDS, and host it on a Web server or a local disk. The UMDS version you use must be of a version compatible with your Update Manager installation. For more information about the compatibility, see Compatibility Between UMDS and the Update Manager Server. You can find the detailed procedure about exporting the upgrades, patch binaries, patch metadata, and notifications in Export the Downloaded Data.
- Required privileges: **VMware vSphere Update Manager.Configure**.

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Download Setings**.

5 In the Download Sources pane, click **Edit**.

   An Edit Download Sources dialog box opens.

6 Select the option **Use a shared repository**.

7 Enter the path or the URL to the shared repository.

   For example, `C:\`*`repository_path`*`\`, `https://`*`repository_path`*`/`, or `http://`*`repository_path`*`/`

   In these examples, *repository_path* is the path to the folder to which you have exported the downloaded upgrades, patches, extensions, and notifications. In an environment where the Update Manager server does not have direct access to the Internet, but is connected to a machine that has Internet access, the folder can be on a Web server.

You can specify an HTTP or HTTPS address, or a location on the disk on which Update Manager is installed. HTTPS addresses are supported without any authentication.

Important You cannot use folders located on a network drive as a shared repository. Update Manager does not download updates from folders on a network share either in the Microsoft Windows Uniform Naming Convention form (such as `\\Computer_Name_or_Computer_IP\Shared`), or on a mapped network drive (for example, `Z:\`).

---

8 Click **OK** to close the Edit Download Sources dialog.

The vSphere Web Client performs validation of the URL.

Important If the updates in the folder you specify are downloaded with a UMDS version that is not compatible with the Update Manager version you use, the validation fails and you receive an error message.

You must make sure that the validation is successful. If the validation fails, Update Manager reports a reason for the failure. You can use the path to the shared repository only when the validation is successful.

9 In the Download Sources pane, click **Download Now** to run the Download patch definitions task.

All notifications and updates are downloaded immediately even if the **Enable scheduled download** check box is selected in **Manage > Notification Check Schedule** or **Manage > Download Schedule**, respectively.

The shared repository is used as a source for downloading upgrades, patches, and notifications.

Example: Using a Folder or a Server as a Shared Repository

You can use a folder or a Web server as a shared repository.

- When you use a folder as a shared repository, *repository_path* is the top-level directory where patches and notifications exported from UMDS are stored.

  For example, export the patches and notifications using UMDS to `F:\` drive, which is a drive mapped to a plugged-in USB device on the machine on which UMDS is installed. Then, plug in the USB device to the machine on which Update Manager is installed. On this machine the device is mapped as `E:\`. The folder to configure as a shared repository in the Update Manager is `E:\`.

- When you use a Web server as a shared repository, *repository_path* is the top-level directory on the Web server where the patches exported from UMDS are stored.

  For example, export the patches and notifications from UMDS to `C:\docroot\exportdata`. If the folder is configured on a Web server and is accessible from other machines at the URL `https://`*`umds_host_name`*`/exportdata`, the URL to configure as a shared repository in Update Manager is `https://`*`umds_host_name`*`/exportdata`.

Import Patches Manually

Instead of using a shared repository or the Internet as a download source for patches and extensions, you can import patches and extensions manually by using an offline bundle.

You can import offline bundles only for hosts that are running ESXi 6.0 or later.

Prerequisites

- The patches and extensions you import must be in ZIP format.
- Required privileges: **VMware vSphere Update Manager.Upload File.Upload File**.

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Download Setings**.

5 In the Download Sources pane, click **Import Patches**.

   The **Import Patches** wizard opens.

6 On the Import Patches page, browse and select the `.zip` file containing the patches you want to import.

7 Click **Upload file** and wait until the file upload completes successfully.

   In case of upload failure, check whether the structure of the `.zip` file is correct, or whether the Update Manager network settings are set up correctly.

8 On the Ready to complete page, review the patches that you have selected to import into the repository.

9 Click **Finish**.

You imported the patches into the Update Manager patch repository. You can view the imported patches on the Update Manager **Patch Repository** tab.

Configure the Update Manager Proxy Settings

You can configure Update Manager to download updates from the Internet using a proxy server.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

  The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Download Setings**.

5 In the Proxy Settings pane, click **Edit**.

6 Select **Use proxy**, and change the proxy information.

7 If the proxy requires authentication, select **Proxy requires authentication**, and provide a user name and password.

8 (Optional) Click **Test Connection** to test that you can connect to the Internet through the proxy.

9 Click **OK**.

You configured Update Manager to use an Internet proxy to download upgrades, patches, extensions, and related metadata.

Configure Checking for Updates

Update Manager checks for host patches, and extensions at regular intervals. Generally, the default schedule settings are sufficient, but you can change the schedule if your environment requires more or less frequent checks.

In some cases you might want to decrease the duration between checks for updates. If you are not concerned about the latest updates and want to reduce network traffic, or if you cannot access the update servers, you can increase the duration between checks for updates.

By default the task to download update metadata and binaries is enabled and is called VMware vSphere Update Manager Update Download task. By modifying this task, you can configure checking for updates.You can modify the VMware vSphere Update Manager Check Notification task in one of the following ways:

- The **Configure** tab of the Update Manager Administration view.
- In the vSphere Web Client, navigate to **Monitor** tab, select the **Tasks & Events** tab, and select **Scheduled Tasks**.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

To download update data, the machine on which Update Manager is installed must have Internet access.

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Download Schedule**.

5 Click **Edit**.

The **Edit Download Schedule** wizard opens.

6 Select **Enable scheduled task** check box, and click **Next**.

If you deselect the check box, the scheduled task that checks for notifications is disabled. However, you can still force a check and download notifications by clicking the **Download Now** button in **Download Settings** pane.

7 Specify a task name and, optionally, a description, or keep the defaults.

8 Click **Change** to specify the time when notification checks run, and click **OK**.

The Configure Scheduler dialog box opens.

Option	Description
Run this action now	Runs the notification check immediately.
Schedule this option to run later	Runs the notification check at the time that you schedule for the task.
Setup a recurring schedule for this action	Runs the notification check recurrently at the frequency, interval, and start time that you schedule for the task.

9 (Optional) Specify one or more email addresses where notifications about patch recalls or email alerts are sent, and click **Next**.

You must configure mail settings for the vSphere Web Client system to enable this option. For more information, see *vCenter Server and Host Management*.

10 Review the Ready to Complete page, and click **Finish**.

The task runs according to the time you specified.

Configuring and Viewing Notifications

At regular time intervals, Update Manager contacts VMware to download information (notifications) about patch recalls, new fixes, and alerts.

In case patches with issues or potential issues are released, the patch metadata is updated, and Update Manager marks the patches as recalled. If you try to install a recalled patch, Update Manager notifies you that the patch is recalled and does not install it on the host. Update Manager notifies you if a recalled patch is already installed on certain hosts. Update Manager also deletes all the recalled patches from the patch repository.

When a patch fixing the problem is released, Update Manager downloads the new patch and prompts you to install it to fix the issues that the recalled patch might cause. If you have already installed a recalled patch, Update Manager alerts you that the patch is recalled and that there is a fix you must install.

Update Manager supports patch recalls for offline bundles that you have imported. Patches from an imported offline bundle are recalled when you import a new offline bundle. The `metadata.zip` file contains information about the patches that must be recalled. Update Manager removes the recalled patches from the patch repository, and after you import a bundle containing fixes, Update Manager notifies you about the fixes and sends email notifications if you have enabled them.

If you use a shared repository as a source for downloading patches and notifications, Update Manager downloads recall notifications from the shared repository to the Update Manager patch repository, but does not send recall email alerts. For more information about using a shared repository, see Use a Shared Repository as a Download Source.

Note After a download of patch recall notifications, Update Manager flags recalled patches but their compliance state does not refresh automatically. You must perform a scan to view the updated compliance state of patches affected by the recall.

Configure Notifications Checks

By default Update Manager checks for notifications about patch recalls, patch fixes, and alerts at certain time intervals. You can modify this schedule.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

To configure notification checks, make sure that the machine on which Update Manager is installed has Internet access.

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Notification Check Schedule**.

5 Click **Edit**.

The **Edit Notifications Check Schedule** wizard opens.

6 Select **Enable scheduled task** check box, and click **Next**.

If you deselect the check box, the scheduled task that checks for notifications is disabled. However, you can still force a check and download notifications by clicking the **Download Now** button in **Download Settings** pane.

7 Specify a task name and, optionally, a description, or keep the defaults.

8 Click **Change** to specify the time when notification checks run, and click **OK**.

The Configure Scheduler dialog box opens.

Option	Description
Run this action now	Runs the notification check immediately.
Schedule this option to run later	Runs the notification check at the time that you schedule for the task.
Setup a recurring schedule for this action	Runs the notification check recurrently at the frequency, interval, and start time that you schedule for the task.

9 (Optional) Specify one or more email addresses where notifications about patch recalls or email alerts are sent, and click **Next**.

You must configure mail settings for the vSphere Web Client system to enable this option. For more information, see *vCenter Server and Host Management*.

10 Review the Ready to Complete page, and click **Finish**.

The task runs according to the time you specified.

View Notifications and Run the Notification Checks Task Manually

Notifications that Update Manager downloads are displayed on the **Notifications** tab of the Update Manager Administration view.

Prerequisites

Connect thevSphere Web Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** icon.

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Monitor** tab.

4 Click the **Notifications** tab.

5 To view the notification details, double-click a notification.

6 To check for notifications immediately, click **Check Notifications** on the upper right of the notifications list.

   You immediately download all new notifications that are available on the VMware website. The notifications are downloaded even if the **Enable scheduled download** check box is not selected in **Manage > Settings > Notification Check Schedule**.

Types of Update Manager Notifications

Update Manager downloads all notifications that are available on the VMware Web site. Some notifications can trigger an alarm. By using the **Alarm Definitions** wizard, you can configure automated actions to be taken when an alarm is triggered.

Notifications appear in the **Notifications** tab that is located under the **Monitor** tab in the Update Manager Admin View.

Information notifications	Information notifications do not trigger an alarm. Clicking an information notification opens the Notification Details window.
Warning notifications	Warning notifications trigger an alarm, which appears in the vSphere Web Client **Alarms** pane. Warning notifications are typically fixes for patch recalls. Clicking a warning notification opens the Patch Recall Details window.
Alert notifications	Alert notifications trigger an alarm, which appears in the vSphere Web Client **Alarms** pane. Alert notifications are typically patch recalls. Clicking an alert notification opens the Patch Recall Details window.

Configuring Host and Cluster Settings

There are several host and cluster settings that you can use to organize the Update Manager behavior during host patch and host upgrade operations.

Host and Cluster Settings

When you update vSphere objects in a cluster with vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), and vSphere Fault Tolerance (FT) enabled, you can temporarily disable vSphere Distributed Power Management (DPM), HA admission control, and FT for the entire cluster. When the update completes, Update Manager restores these features.

Updates might require the host to enter maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure availability, vCenter Server can migrate virtual machines to other ESXi hosts within the cluster before the host is put into maintenance mode. vCenter Server migrates the virtual machines if the cluster is configured for vSphere vMotion, and if DRS is enabled.

Enable Enhanced vMotion Compatibility (EVC) to help ensure vSphere vMotion compatibility between the hosts in the cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. Use of EVC prevents migrations with vSphere vMotion from failing because of incompatible CPUs. You can enable EVC only in a cluster where host CPUs meet the compatibility requirements. For more information about EVC and the requirements that the hosts in an EVC cluster must meet, see *vCenter Server and Host Management*.

If a host has no running virtual machines, DPM might put the host in standby mode and interrupt an Update Manager operation. To make sure that scanning and staging complete successfully, Update Manager disables DPM during these operations. To ensure a successful remediation, have Update Manager disable DPM and HA admission control before the remediation operation. After the operation completes, Update Manager restores DPM and HA admission control. Update Manager disables HA admission control before staging and remediation but not before scanning.

If DPM has already put hosts in standby mode, Update Manager powers on the hosts before scanning, staging, and remediation. After the scanning, staging, or remediation is complete, Update Manager turns on DPM and HA admission control and lets DPM put hosts into standby mode, if needed. Update Manager does not remediate powered off hosts.

If hosts are put into standby mode and DPM is manually disabled for a reason, Update Manager does not remediate or power on the hosts.

Within a cluster, temporarily disable HA admission control to let vSphere vMotion to proceed. This action prevents downtime of the machines on the hosts that you remediate. After the remediation of the entire cluster, Update Manager restores HA admission control settings.

If FT is turned on for any of the virtual machines on hosts within a cluster, temporarily turn off FT before performing any Update Manager operations on the cluster. If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. Remediate all hosts in a cluster with the same updates, so that FT can be reenabled after the remediation. A primary virtual machine and a secondary virtual machine cannot reside on hosts of different ESXi version and patch levels.

Host and Cluster Settings with Effect on vSAN Clusters

As you remediate hosts that are part of a vSAN cluster, be aware of the following behavior:

- The host remediation process might take an extensive amount of time to complete.
- By design, only one host from a vSAN cluster can be in a maintenance mode at any time.
- Update Manager remediates hosts that are part of a vSAN cluster sequentially even if you set the option to remediate the hosts in parallel.
- If a host is a member of a vSAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because vSAN has to migrate the virtual machine data from one disk to another in the vSAN datastore cluster. Delays might take up to hours. You can work around this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the vSAN datastore.

Quick Boot Setting for Optimizing Host Patch and Host Upgrade Operations

Quick Boot of an ESXi host is a setting that lets Update Manager optimize the remediation time of hosts that undergo patch and upgrade operations. A patch or upgrade operation does not affect the hardware of a host. If the Quick Boot feature is enabled, Update Manager skips the hardware reboot (the BIOS or UEFI firmware reboot). As a result, the time an ESXi host spends in Maintenance Mode shortens and the risk of failures during remediation is minimized.

System Requirements for Using Quick Boot During Remediation

The Quick Boot of ESXi hosts is an option that allows Update Manager to reduce the time a host remediation takes by skipping the physical reboot of the host.

Using Quick Boot is supported with a limited set of hardware platforms, drivers, and is not supported on ESXi hosts that use TPM or passthru devices. For more information about a host compatibility to Quick Boot option, see the following KB Article: https://kb.vmware.com/s/article/52477.

Configure Using Quick Boot During Host Remediation

Configure Update Manager to reduce the remediation time during host patch or host upgrade operations.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Configure**
- Verify your ESXi hosts environment is compatible with Quick Boot. See System Requirements for Using Quick Boot During Remediation.

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Host/Cluster Settings**.

5 Click **Edit**.

   The Edit Host/Cluster Settings dialog box opens.

6 Select **Enable Quick Boot** check box to allow Update Manager to reduce the host reboot time during remediation.

7 Click **OK**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Configure Host Maintenance Mode Settings

ESXi host updates might require that the host enters maintenance mode before they can be applied. Update Manager puts the ESXi hosts in maintenance mode before applying these updates. You can configure how Update Manager responds if the host fails to enter maintenance mode.

For hosts in a container different from a cluster or for individual hosts, migration of the virtual machines with vMotion cannot be performed. If vCenter Server cannot migrate the virtual machines to another host, you can configure how Update Manager responds.

Hosts that are part of a vSAN cluster can enter maintenance mode only one at a time. This is a specificity of the vSAN clusters.

If a host is a member of a vSAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because vSAN has to migrate the virtual machine data from one disk to another in the vSAN datastore cluster. Delays might take up to hours. You can work around this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the vSAN datastore.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Host/Cluster Settings**.

5 Click **Edit**.

   The Edit Host/Cluster Settings dialog box opens.

6 Under Host Settings, select an option from the **VM Power state** drop-down menu to determine the change of the power state of the virtual machines that run on the host to be remediated.

The option that you select determines how the power state changes for the virtual machines that run on the host when the host enters maintenance mode before remediation.

Option	Description
Power Off virtual machines	Powers off all virtual machines before remediation.
Suspend virtual machines	Suspends all running virtual machines before remediation.
Do Not Change VM Power State	Leaves virtual machines in their current power state. This is the default setting.

7 (Optional) Select **Retry entering maintenance mode in case of failure**, and specify the retry delay, and the number of retries.

If a host fails to enter maintenance mode before remediation, Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries**.

8 (Optional) Select **Temporarily disable any removable media devices that might prevent a host from entering maintenance mode**.

Update Manager does not remediate hosts on which virtual machines have connected CD/DVD or floppy drives. All removable media drives that are connected to the virtual machines on a host might prevent the host from entering maintenance mode and interrupt remediation.

After remediation, Update Manager reconnects the removable media devices if they are still available.

9 Click **OK**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Configure Cluster Settings

For ESXi hosts in a cluster, the remediation process can run either in a sequence or in parallel. Certain features might cause remediation failure. If you have VMware DPM, HA admission control, or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

Note Remediating hosts in parallel can improve performance significantly by reducing the time required for cluster remediation. Update Manager remediates hosts in parallel without disrupting the cluster resource constraints set by DRS. Avoid remediating hosts in parallel if the hosts are part of a vSAN cluster. Due to the specifics of the vSAN cluster, a host cannot enter maintenance mode while other hosts in the cluster are currently in maintenance mode.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click **Settings**, and select **Host/Cluster Settings**.

5 Click **Edit**.

The Edit Host/Cluster Settings dialog box opens.

6 Under Cluster Settings, select the check boxes for options that you want to disable or enable.

Option	Description
Distributed Power Management (DPM)	VMware DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state. If you do not choose to disable DPM, Update Manager skips the cluster on which VMware DPM is enabled. If you choose to temporarily disable VMware DPM, Update Manager disables DPM on the cluster, remediates the hosts in the cluster, and re-enables VMware DPM after remediation is complete.
High Availability (HA) admission control	Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion. If you do not choose to disable HA admission control, Update Manager skips the cluster on which HA admission control is enabled. If you choose to temporarily disable HA admission control, Update Manager disables HA admission control, remediates the cluster, and re-enables HA admission control after remediation is complete.
Fault Tolerance (FT)	FT provides continuous availability for virtual machines by automatically creating and maintaining a secondary virtual machine that is identical to the primary virtual machine. If you do not choose to turn off FT for the virtual machines on a host, Update Manager does not remediate that host.
Enable parallel remediation for hosts in cluster	Update Manager can remediate hosts in clusters in a parallel manner. Update Manager continuously evaluates the maximum number of hosts it can remediate in parallel without disrupting DRS settings. If you do not select the option, Update Manager remediates the hosts in a cluster sequentially. By design only one host from a vSAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a vSAN cluster sequentially even if you select the option to remediate them in parallel.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can select to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

7 Click **OK**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Enable Remediation of PXE Booted ESXi Hosts

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

The global setting in the Update Manager **Configuration** tab enables solutions such as ESX Agent Manager or Cisco Nexus 1000V to initiate remediation of PXE booted ESXi hosts. In contrast, the **Enable patch remediation of powered on PXE booted ESXi hosts** setting in the **Remediate** wizard enables Update Manager to patch PXE booted hosts.

To retain updates on stateless hosts after a reboot, use a PXE boot image that contains the updates. You can update the PXE boot image before applying the updates with Update Manager, so that the updates are not lost because of a reboot. Update Manager itself does not reboot the hosts because it does not install updates requiring a reboot on PXE booted ESXi hosts.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1. In the Home view of the vSphere Web Client, select the Update Manager icon.
2. From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
3. Click the **Manage** tab.
4. Click **Settings**, and select **Host/Cluster Settings**.
5. Click **Edit**.

   The Edit Host/Cluster Settings dialog box opens.
6. Under Host Settings, select **Allow installation of additional software on PXE booted ESXi hosts**.

   Selecting this option enables installation of software for solutions on PXE booted ESXi hosts in the vSphere inventory that you manage with this Update Manager instance.
7. Click **OK**.

Take Snapshots Before Remediation

By default, Update Manager is configured to take snapshots of virtual machines before applying updates. If the remediation fails, you can use the snapshot to return the virtual machine to the state before the remediation.

Update Manager does not take snapshots of fault tolerant virtual machines and virtual machines that are running virtual machine hardware version 3. If you decide to take snapshots of such virtual machines, the remediation might fail.

You can choose to keep snapshots indefinitely or for a fixed period. Use the following guidelines when managing snapshots:

- Keeping snapshots indefinitely might consume a large amount of disk space and degrade virtual machine performance.
- Keeping no snapshots saves space, ensures best virtual machine performance, and might reduce the amount of time it takes to complete remediation, but limits the availability of a rollback.
- Keeping snapshots for a set period uses less disk space and offers a backup for a short time.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.
2 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
3 Click the **Manage** tab.
4 Click **Settings**, and select **VM Settings**.
5 Click **Edit**.

   The Edit VM Settings dialog box opens.
6 To enable or disable taking of snapshots of virtual machines before remediating them, select the **Take a snapshot of the virtual machines before remediation to enable rollback** check box.

   The option to take snapshots is selected by default.
7 Configure snapshots to be kept indefinitely or for a fixed period.
8 Click **Apply**.

These settings become the default rollback option settings for virtual machines. You can specify different settings when you configure individual remediation tasks.

Configure Smart Rebooting

Smart rebooting selectively restarts the virtual machines in the vApp to maintain startup dependencies. You can enable and disable smart rebooting of virtual machines in a vApp after remediation.

A vApp is a prebuilt software solution, consisting of one or more virtual machines and applications, which are potentially operated, maintained, monitored, and updated as a unit.

Smart rebooting is enabled by default. If you disable smart rebooting, the virtual machines are restarted according to their individual remediation requirements, disregarding existing startup dependencies.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Configure**

Procedure

1. In the Home view of the vSphere Web Client, select the Update Manager icon.
2. From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
3. Click the **Manage** tab.
4. Click **Settings**, and click **vApp Settings**.
5. Click **Edit**.

   The vApp Settings dialog box opens.
6. Click the **Enable smart reboot after remediation** check box to enable or disable smart rebooting.

Configure the Update Manager Patch Repository Location

When you install Update Manager, you can select the location for storing the downloaded patches and upgrade binaries. To change the location after installation, you must manually edit the `vci-integrity.xml` file.

Procedure

1. Log in as an administrator to the machine on where Update Manager server runs.
2. Stop the Update Manager service.
   a. Right-click **My Computer** and click **Manage**.
   b. In the left pane, expand **Services and Applications**, and click **Services**.
   c. In the right pane, right-click **VMware vSphere Update Manager Service** and click **Stop**.
3. Navigate to the Update Manager installation directory and locate the `vci-integrity.xml` file.

   The default location is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.
4. (Optional) In case you want to revert to the previous configuration, create a backup copy of this file.
5. Edit the file by changing the following items:

```
<patchStore>your_new_location</patchStore>
```

The default patch download location is `C:\Documents and Settings\All Users\Application Data\VMware\VMware Update Manager\Data\`.

The directory path must end with `\`.

6 Save the file in UTF-8 format, replacing the existing file.

7 Copy the contents from the old patch store directory to the new folder.

8 Start the Update Manager service by right-clicking **VMware vSphere Update Manager Service** in the **Computer Management** window and selecting **Start**.

Run the VMware vSphere Update Manager Update Download Task

If you change the patch download source settings, you must run the VMware vSphere Update Manager Update Download task to download any new patches, extensions, and notifications.

Procedure

1 In the vSphere Web Client, select an inventory object, and select the **Monitor** tab.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, specify the Update Manager instance to configure.

2 Click the **Task & Events** tab, and select **Scheduled Tasks**.

3 Right-click the **VMware vSphere Update Manager Update Download** task, and select **Run**.

You can see the running task listed in the **Recent Tasks** pane.

Update Manager Privileges

To configure Update Manager settings, to manage baselines, patches, and upgrades, you must have the proper privileges. You can assign Update Manager privileges to different roles from the vSphere Web Client.

Update Manager privileges cover distinct functionalities.

Table 5-3. Update Manager Privileges

Privilege Group	Privilege	Description
Configure	**Configure Service**	Configure the Update Manager service and the scheduled patch download task.
Manage Baseline	**Attach Baseline**	Attach baselines and baseline groups to objects in the vSphere inventory.
	Manage Baseline	Create, edit, or delete baseline and baseline groups.

Table 5-3. Update Manager Privileges (Continued)

Privilege Group	Privilege	Description
Manage Patches and Upgrades	**Remediate to Apply Patches, Extensions, and Upgrades**	Remediate virtual machines and hosts to apply patches, extensions, or upgrades. In addition, this privilege allows you to view compliance status.
	Scan for Applicable Patches, Extensions, and Upgrades	Scan virtual machines and hosts to search for applicable patches, extensions, or upgrades.
	Stage Patches and Extensions	Stage patches or extensions to hosts. In addition, this privilege allows you to view compliance status of the hosts.
	View Compliance Status	View baseline compliance information for an object in the vSphere inventory.
Upload File	**Upload File**	Upload upgrade images and offline patch bundles.

For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*.

Installing, Setting Up, and Using Update Manager Download Service 6

VMware vSphere Update Manager Download Service (UMDS) is an optional module of Update Manager. UMDS downloads patch metadata, patch binaries, and notifications that would not otherwise be available to the Update Manager server.

For security reasons and deployment restrictions, vSphere, including Update Manager, might be installed in a secured network that is disconnected from other local networks and the Internet. Update Manager requires access to patch information to function properly. If you are using such an environment, you can install UMDS on a computer that has Internet access to download upgrades, patch binaries, and patch metadata, and then export the downloads to a portable media drive so that they become accessible to the Update Manager server.

In a deployment where the machine on which Update Manager is installed has no Internet access, but is connected to a server that has Internet access, you can automate the export process and transfer files from UMDS to the Update Manager server by using a Web server on the machine on which UMDS is installed.

UMDS 6.7 supports patch recalls and notifications. A patch is recalled if the released patch has problems or potential issues. After you download patch data and notifications with UMDS, and export the downloads so that they become available to the Update Manager server, Update Manager deletes the recalled patches and displays the notifications on the Update Manager **Notifications** tab. For more information about patch recalls and notifications, see Configuring and Viewing Notifications.

With Update Manager release 6.7, the UMDS is available for installation on Windows and Linux-based operating systems. The machine on which you install UMDS must have Internet access.

For UMDS that runs on Windows, only Administrator or users that are part of the Administrators group can download patches. Administrator access is not a requirement for downloading patches with UMDS that runs on Linux.

This chapter includes the following topics:

Compatibility Between UMDS and the Update Manager Server

UMDS must be of a version that is compatible with the Update Manager server.

Update Manager can work with a certain UMDS version if the metadata and structure of the patch store that UMDS exports is compatible with Update Manager, and if the data can be imported and used by the Update Manager server.

UMDS 6.7 is compatible and can work only with Update Manager 6.7.

Installing UMDS on a Windows Operating System

You can install and use UMDS to download patch binaries, patch metadata, and notifications if Update Manager does not have access to the Internet. The machine on which you install UMDS must have Internet access.

Note You cannot upgrade UMDS 6.0 or UMDS 6.5 to UMDS 6.7. You can perform a fresh installation of UMDS 6.7 according to all system requirements, and use an existing patch store from UMDS 6.0 or UMDS 6.5. You can install UMDS only on 64-bit machines.

Before installing UMDS, you must create a supported database instance, configure a 64-bit DSN, and test the DSN from ODBC. If you are using the bundled Microsoft SQL Server 2012 Express, you can install and configure the database when you install UMDS.

Installing UMDS 6.7 in an Environment With Update Manager 6.7 Instances Only

In the UMDS 6.7 installation wizard for Windows, you can select the patch store to be an existing download directory from an earlier UMDS 6.0 or UMDS 6.5 installation and reuse the applicable downloaded updates in UMDS 66.7. You must uninstall existing UMDS 6.0 or UMDS 6.5 instances before reusing the patch store. Once you associate an existing download directory with UMDS 6.7, you cannot use it with earlier UMDS versions.

If you install UMDS with an existing download directory, make sure that you perform at least one download by using UMDS 6.7 before you export updates.

Installing UMDS 6.7 in an Environment With Both Update Manager 6.0 and Update Manager 6.7 Instances

You must not install UMDS 6.7 with an existing UMDS 6.5 download directory if your environment contains both Update Manager 6.5 and Update Manager 6.7 instances. In such a case, you need a UMDS 6.5 and a UMDS 6.7 installation on two separate machines, so that you can export updates for the respective Update Manager versions.

Regardless of the version, you must not install the UMDS on the same machine as the Update Manager server.

Install UMDS on a Windows Operating System

Install UMDS if the machine on which Update Manager is installed does not have access to the Internet.

Prerequisites

- Verify that the machine on which you install UMDS has Internet access, so that UMDS can download upgrades, patch metadata, and patch binaries.
- Uninstall any 6.5 or earlier instance of UMDS if it is installed on the machine. If such a version of UMDS is already installed, the installation wizard displays an error message and the installation cannot proceed.
- Before you install UMDS, create a database instance and configure it. If you install UMDS on a 64-bit machine, you must configure a 64-bit DSN and test it from ODBC. The database privileges and preparation steps are the same as the ones used for Update Manager. For more information, see Preparing the Update Manager Database.
- If you plan to use the bundled Microsoft SQL Server 2012 Express database, make sure that you install Microsoft Windows Installer version 4.5 (MSI 4.5) on your system.
- UMDS and Update Manager must be installed on different machines.
- To ensure optimal performance, install UMDS on a system with requirements same as the ones for the Update Manager server listed in System Requirements.
- Update Manager installation requires installation of the Microsoft .NET framework 4.7. Consider the following before proceeding with the installation.
  - Installing Microsoft .NET framework 4.7 is not supported on Microsoft Windows Server 2008 Service Pack 2 64-bit.
  - Installing Microsoft .NET framework 4.7 might require you to install some additional Windows updates. Relevant links to the Windows updates are provided during the Microsoft .NET framework 4.7.
  - Installing Microsoft .NET framework 4.7 might require you to reboot your host operating system.
  - If you plan to install Update Manager server on the same Windows machine where vCenter Server runs (typical installation), the vCenter Server service might temporarily disconnect if the a reboot is invoked on the system by the .NET Microsoft .NET framework 4.7 installation.
  - After installing or upgrading the Microsoft .NET framework 4.7, follow the prompts of the Update Manager server or the UMDS installation wizards.

Procedure

1. Mount the ISO image of the vCenter Server installer to the Windows virtual machine or physical server on which you want to install the vSphere Update Manager Download Service (UMDS).
2. In the mounted directory, double-click the `autorun.exe` file of the **VMware vCenter Installer**, and select **vSphere Update Manager > Download Service**.

3 (Optional) Select the option to **Use Microsoft SQL Server 2012 Express as the embedded database**, and click **Install**.

Note Skip this step only if you plan to use another supported Oracle or SQL Server database.

If the Microsoft SQL Server 2012 Express is not present on your system from previous Update Manager installations, the installation wizard for the Microsoft SQL Server 2012 Express opens.

4 Select the option to install the Microsoft .NET framework 4.7.

Note If you do not select to install Microsoft .NET framework 4.7, the Update Manager Download Service installation will fail with an error message.

5 On the **VMware vCenter Installer**, click **Install**.

The **VMware vCenter Installer** wizard remains open, and a language selection dialog box opens.

6 Select the language for the **vSphere Update Manager Download Service** installer, and click **OK**.

7 Depending on the database selection you made in the **VMware vCenter Installer**, perform one of the following steps:

- If you selected to use embedded Microsoft SQL Server 2012, wait for the installation process of the Microsoft .NET framework 4.7 and the Microsoft SQL Server 2012 to complete, and from the VMware vCenter Installer, click **Install** again.

  The VMware vSphere Update Manager Download Service installer opens.

- If you are using another supported database and did not select to use the embedded Microsoft SQL Server 2012, the VMware vSphere Update Manager Download Service installer opens, and you can proceed with next steps.

8 (Optional) If the wizard prompts you, install the required items such as Windows Installer 4.5.

This step is required only if Windows Installer 4.5 is not present on your machine and you must perform it the first time you install a vSphere 5.x product. After the system restarts, the installer starts again.

9 Review the Welcome page and click **Next**.

10 Read and accept the license agreement, and click **Next**.

11 Accept the terms in the license agreement and click **Next**.

12 (Optional) Select the database, and click **Next**.

If you selected to use the embedded Microsoft SQL Server 2012 Express database, the installation wizard skips this page.

a Use an existing supported database, by selecting your database from the list of DSNs. If the DSN does not use Windows NT authentication, enter the user name and password for the DSN and click **Next**.

Important The DSN must be a 64-bit DSN.

13 Enter the Update Manager Download Service proxy settings and click **Next**.

14 Select the Update Manager Download Service installation and patch download directories and click **Next**.

If you do not want to use the default locations, you can click **Change** to browse to a different directory. You can select the patch store to be an existing download directory from a previous UMDS 6.0 or UMDS 6.5 installation and reuse the applicable downloaded updates in UMDS 6.7. After you associate an existing download directory with UMDS 6.7, you cannot use it with earlier UMDS versions.

15 (Optional) In the warning message about the disk free space, click **OK**.

16 Click **Install** to begin the installation.

17 Click **OK** in the Warning message notifying you that .NET Framework 4.7 is not installed.

The UMDS installer installs the prerequisite before the actual product installation.

18 Click **Finish**.

UMDS is installed.

Installing and Upgrading UMDS on a Linux-Based Operating System

In vSphere 6.7 release, the UMDS 6.7 is bundled with the vCenter Server Appliance 6.7. You can use the UMDS bundle from the vCenter Server Appliance to install UMDS 6.7 on a separate Linux-based system.

UMDS is a 64-bit application and requires a 64-bit Linux-based system.

You cannot upgrade UMDS that runs on a Linux-based operating system. You can uninstall the current version of UMDS, perform a fresh installation of UMDS according to all system requirements, and use the existing patch store from the UMDS that you uninstalled.

A UMDS that you install on a Linux-based operating system requires PostgreSQL database.

Supported Linux-Based Operating Systems and Databases for Installing UMDS

The Update Manager Download Service (UMDS) can run on a limited number of Linux-based operating systems in combination with a particular database format.

The supported combinations of a Linux-based operating system and a database that can run UMDS are as follows:

- Ubuntu 14.0.4 with PostgreSQL database 9.3.11.
- Red Hat Enterprise Linux 7.0 with PostgreSQL database 9.2.

Configure PostgreSQL Database for UMDS on Linux

Install and configure a PostgreSQL database instance on the Linux-based machine where you plan to install Update Manager Download Service (UMDS).

Prerequisites

- Verify PostgreSQL database instance of a supported version is installed on the system, and that the Linux system is also of a supported type. See Supported Linux-Based Operating Systems and Databases for Installing UMDS
- Verify you have PostgreSQL database user credentials.
- Verify that the UMDS installation directory is different from the patch store directory.

Procedure

1 In the Linux machine, open the Command Shell.

2 Log in as a PostgreSQL user, and create a database instance and a database user, by running the following commands:

```
su - postgres
createdb <database_name>
createuser -d -e -r <database_username> -P
Pwd: <database_password>
```

3 Navigate to the folder that contains the PostgreSQL configuration file `pg_hba.conf`.

Linux system	Default Location
Ubuntu 14.0.4	`/etc/postgresql/<postgres_version>/main/pg_hba.conf`
Red Hat Enterprise Linux 7.0	`/var/lib/pgsql/<postgres_version>/data/pg_hba.conf`

4 In the PostgreSQL configuration file, enable password authentication for the database user by inserting the following line right above `local all all peer`.

#TYPE	DATABASE	USER	ADDRESS	METHOD
local	*<database_name>*	*<database_username>*		md5

5 Log out as a PostgreSQL user, by running the following command:

```
logout
```

6 Create a configuration file `/etc/odbcinst.ini`.

7 Depending on the Linux system, navigate to the ODBC driver files `psqlodbcw.so` or `libodbcpsqlS.so`.

Linux system	Default Location
Ubuntu 14.0.4	`/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so`
Red Hat Enterprise Linux 7.0	`/usr/lib64/libodbcpsqlS.so`

8 Add driver paths files to `/etc/odbcinst.ini`.

Linux system	Command
Ubuntu 14.0.4	[PostgreSQL] Description=PostgreSQL ODBC driver (Unicode version) Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so Debug=0 CommLog=1 UsageCount=1
Red Hat Linux 7.0	[PostgreSQL] Description=PostgreSQL ODBC driver (Unicode version) Driver64=<path>/psqlodbcw.so Setup64=<path>/libodbcpsqlS.so Debug=0 CommLog=1 UsageCount=1

9 Create a system file `/etc/odbc.ini`.

10 Add the following content to `/etc/odbc.ini`.

```
[UMDS_DSN]
;DB_TYPE = PostgreSQL
;SERVER_NAME = localhost
;SERVER_PORT = 5432
;TNS_SERVICE = <database_name>
;USER_ID = <database_username>
Driver = PostgreSQL
DSN = UMDS_DSN
ServerName = localhost
PortNumber = 5432
Server = localhost
```

```
Port = 5432
UserID = <database_username>
User = <database_username>
Database = <database_name>
```

11 Create a symbolic link between the UMDS and the PostgreSQL, by running the following command:

```
ln -s /var/run/postgresql/.s.PGSQL.5432 /tmp/.s.PGSQL.5432
```

What to do next

When installing UMDS on a Linux-based system, use the PostgreSQL database instance that you configured here.

Install UMDS on a Linux OS

If the vCenter Server Appliance 6.7 in which Update Manager runs does not have access to the Internet, you can install UMDS on a Linux-based operating system to download patch binaries and metadata.

Prerequisites

- Verify you have administrative privileges on the Linux machine where you install the UMDS.
- Install and configure a PostgreSQL database on the Linux machine.
- Mount the ISO file of the vCenter Server Appliance 6.7 to the Linux machine.

Procedure

1 In the Linux machine, open the Command Shell.

2 From the vCenter Server Appliance ISO that you mounted to the Linux machine, copy the `VMware-UMDS-6.7.0.-`*`build_number`*`.tar.gz` file to the Linux machine.

3 Unarchive the `VMware-UMDS-6.7.0.-`*`build_number`*`.tar.gz` file, and navigate to the newly extracted directory `/vmware-umds-distrib`.

   For example, if you unarchived the `VMware-UMDS-6.7.0.-`*`build_number`*`.tar.gz` file, to a directory you created with the name *umds*, your navigation path is `/`*`umds`*`/vmware-umds-distrib`.

4 Run the file UMDS installation script.

   The script has the following filename: `vmware-install.pl`.

5 Read and accept the EULA.

6 Select a directory where to install the UMDS.

7 Enter the UMDS proxy settings.

   You can also change proxy configuration after you install UMDS by using the following command:

```
vmware-umds -S --proxy <proxyAddress:port>
```

8 Select a directory where to store the patches.

Important The patch store directory must be different from the UMDS installation directory.

9 Select the database.

a Provide the database DSN.

b Provide the database user name.

c Provide the database password.

The database is overridden with tables required by the Update Manager Download Service.

UMDS is installed.

Uninstall UMDS from a Linux OS

To use the latest version of the Update Manager Download Service (UMDS) on your Linux-based system, first you must uninstall the current version of UMDS. No direct upgrade path is available to a later version of UMDS, which runs on a Linux-based system.

Prerequisites

- Verify you have administrative privileges on the Linux machine where UMDS runs.

Procedure

1 In the Linux machine, open the Command Shell.

2 Navigate to the UMDS installation directory, and locate the file `vmware-uninstall-umds.pl`.

3 Run the following command:

```
./vmware-uninstall-umds.pl
```

4 To confirm that you want to uninstall UMDS from the system, enter **Yes**.

The UMDS uninstallation procedure starts.

UMDS is uninstalled from the Linux system.

What to do next

You can upgrade your Linux OS, and install a later compatible version of UMDS.

Setting Up and Using UMDS

You can set up UMDS to download patches and notifications for ESXi hosts. You can also set up UMDS to download ESXi 6.0, ESXi 6.5, and ESXi 6.7 patch binaries, patch metadata, and notifications from third-party portals.

For UMDS that runs on Windows, only Administrator or users that are part of the Administrators group can download patches. Administrator access is not a requirement for downloading patches with UMDS that runs on Linux.

After you download the upgrades, patch binaries, patch metadata, and notifications, you can export the data to a Web server or a portable media drive and set up Update Manager to use a folder on the Web server or the media drive (mounted as a local disk) as a shared repository.

You can also set up UMDS to download ESXi 6.0, ESXi 6.5, and ESXi 6.7 patches and notifications from third-party portals.

To use UMDS, the machine on which you install it must have Internet access. After you download the data you want, you can copy it to a local Web server or a portable storage device, such as a CD or USB flash drive.

The best practice is to create a script to download the patches manually and set it up as a Windows Scheduled Task that downloads the upgrades and patches automatically.

Set Up the Data to Download with UMDS

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. You can specify which patch binaries and patch metadata to download with UMDS.

Procedure

1 Log in to the machine where UMDS is installed, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

- The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.
- The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Specify the updates to download.

- To set up a download of all ESXi host updates run the following command:

```
vmware-umds -S --enable-host
```

- To disable the download of host updates, run the following command:

```
vmware-umds -S --disable-host
```

What to do next

Download the selected data.

Change the UMDS Patch Repository Location

UMDS downloads upgrades, patch binaries, patch metadata, and notifications to a folder that you can specify during the UMDS installation.

The default folder to which UMDS downloads patch binaries and patch metadata on a Windows machine is `C:\Documents and Settings\All Users\Application Data\VMware\VMware Update Manager\Data`.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds` .

You can change the folder in which UMDS downloads data after you install UMDS.

If you have already downloaded any host updates, make sure that you copy all the files and folders from the old location to the new patch store location. The folder in which UMDS downloads patch binaries and patch metadata must be located on the machine on which UMDS is installed.

Procedure

1 Log in as an administrator to the machine where UMDS is installed, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   - The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.
   - The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Change the patch repository directory by running the command:

   ```
   vmware-umds -S --patch-store your_new_patchstore_folder
   ```

   In this example, *`your_new_patchstore_folder`* is the path to the new folder in which you want to download the patch binaries and patch metadata.

You successfully changed the directory in which UMDS stores patch data.

What to do next

Download data using UMDS.

Configure URL Addresses for Hosts

You can configure UMDS to connect to the websites of third-party vendors to download ESXi 6.0, ESXi 6.5, and ESXi 6.7 host patches and notifications.

Procedure

1 Log in to the machine where UMDS runs, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   - The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.
   - The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Configure UMDS to download data from the new URL address.

- To add a new URL address for downloading patches and notifications for ESXi 6.0, ESXi 6.5, or ESXi 6.7 hosts, run the following command:

```
vmware-umds -S --add-url https://host_URL/index.xml --url-type HOST
```

4 (Optional) Remove a URL address, so that UMDS does not download data from it anymore.

Downloaded data is retained and can be exported.

- If you are using UMDS on a Windows machine, use the following command:

```
vmware-umds.exe -S --remove-url https://URL_to_remove/index.xml
```

- If you are using UMDS on a Linux machine, use the following command:

```
vmware-umds -S --remove-url https://URL_to_remove/index.xml
```

You configured UMDS to download host patches and notifications from specific URL addresses.

What to do next

Download the patches and notifications by using UMDS.

Download the Specified Data Using UMDS

After you set up UMDS, you can download upgrades, patches and notifications to the machine on which UMDS is installed.

Prerequisites

- If you are using UMDS on Windows, log in as an Administrator, or a user that belongs to the Administrators group. Administrator level access is not a requirement for downloading data with UMDS that runs on Linux.

Procedure

1 Log in to the machine where UMDS is installed, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

- The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.
- The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Download the selected updates.

```
vmware-umds -D
```

This command downloads all the upgrades, patches and notifications from the configured sources for the first time. Subsequently, it downloads all new patches and notifications released after the previous UMDS download.

4 (Optional) If you have already downloaded upgrades, patches, and notifications and want to download them again, you can include the start and end times to restrict the data to download.

The command to re-download patches and notifications deletes the existing data from the patch store (if present) and re-downloads it.

To re-download the upgrades, patches and notifications that were downloaded in November 2010, for example, run the following command:

```
vmware-umds -R --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59
```

The data previously downloaded for the specified period is deleted and downloaded again.

What to do next

Export the downloaded upgrades, patches, and notifications.

Export the Downloaded Data

You can export downloaded upgrades, patches, and notifications to a specific location that serves as a shared repository for Update Manager. You can configure Update Manager to use the shared repository as a patch download source. The shared repository can also be hosted on a Web server.

Prerequisites

- If you are using UMDS on Windows, log in as an Administrator, or a user that belongs to the Administrators group. Administrator level access is not a requirement for exporting the downloaded data with UMDS that runs on Linux.
- If you installed UMDS with an existing download directory, make sure that you perform at least one download by using UMDS 6.7 before you export updates.

Procedure

1 Log in to the machine where UMDS is installed and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   - The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.
   - The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Specify the export parameters and export the data.

```
vmware-umds -E --export-store repository_path
```

In the command, you must specify the full path of the export directory.

If you are working in a deployment in which the Update Manager server is installed on a machine connected to the machine on which UMDS is installed, *repository_path* can be the path to the folder on the Web server that serves as a shared repository.

If the Update Manager server is installed on a machine in an isolated and secure environment, *repository_path* can be the path to a portable media drive. Export the downloads to the portable media drive to physically transfer the patches to the machine on which Update Manager is installed.

The data you downloaded by using UMDS is exported to the path you specify. Make sure that all files are exported. You can periodically perform export from UMDS and populate the shared repository so that Update Manager can use the new patch binaries and patch metadata.

4 (Optional) You can export the ESXi patches that you downloaded during a specified time window.

For example, to export the patches downloaded in November 2010, run the following command:

```
vmware-umds -E --export-store repository-path --start-time 2010-11-01T00:00:00 --end-time
2010-11-30T23:59:59
```

What to do next

Configure Update Manager to use a shared repository as a patch download source. For more information, see Use a Shared Repository as a Download Source.

Working with Baselines and Baseline Groups

7

Update Manager baselines are hosts baselines and virtual machine baselines. To upgrade objects in your vSphere inventory, you can use predefines baselines, system-managed baselines, or custom baselines that you create.

When you scan hosts and virtual machines you evaluate them against baselines and baseline groups to determine their level of compliance.

In the vSphere Web Client, the baselines and baseline groups are displayed on the **Host Baselines** and **VMs Baselines** tabs of the Update Manager Admin view.

Depending on the purpose for which you want to use them, host baselines can contain a collection of one or more patches, extensions, or upgrades. Therefore host baselines are upgrade, extension, or patch baselines. To update or upgrade your hosts you can use the Update Manager default baselines, or custom baselines that you create.

The VMs baselines are predefined. You cannot create custom VMs baselines.

The default baselines are the predefined and system managed baselines.

System Managed Baselines

The Update Manager displays system managed baselines that are generated by vSAN. These baselines appear by default when you use vSAN clusters with ESXi hosts of version 6.0 Update 2 and later in your vSphere inventory. If your vSphere environment does not contain any vSAN clusters, no system managed baselines are created.

The system managed baselines automatically update their content periodically, which requires Update Manager to have constant access to the Internet. The vSAN system baselines are typically refreshed every 24 hours.

You can use the system managed baselines to upgrade your vSAN clusters to recommended critical patches, drivers, updates or latest supported ESXi host version for vSAN.

Predefined Baselines

Predefined baselines cannot be edited or deleted, you can only attach or detach them to the respective inventory objects.

Under the **Host Baselines** tab in Update Manager Admin view, you can see the following predefined baselines:

Critical Host Patches (Predefined)	Checks ESXi hosts for compliance with all critical patches.
Non-Critical Host Patches (Predefined)	Checks ESXi hosts for compliance with all optional patches.

Under the **VMs Baselines** tab in Update Manager Admin view, you can see the following predefined baselines:

VMware Tools Upgrade to Match Host (Predefined)	Checks virtual machines for compliance with the latest VMware Tools version on the host. Update Manager supports upgrading of VMware Tools for virtual machines on hosts that are running ESXi 6.0.x and later.
VM Hardware Upgrade to Match Host (Predefined)	Checks the virtual hardware of a virtual machine for compliance with the latest version supported by the host. Update Manager supports upgrading to virtual hardware version vmx-14 on hosts that are running ESXi 6.7.

Custom Baselines

Custom baselines are the baselines you create.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain and you have an Update Manager instance for each vCenter Server system in the group, the baselines and baseline groups you create and manage are applicable only to inventory objects managed by the vCenter Server system with which the selected Update Manager instance is registered. You can use an Update Manager instance only with a vCenter Server system with which the instance is registered.

Baseline Groups

Baseline groups are assembled from existing baselines. A baseline group might contain one upgrade baseline, and one or more patch and extension baselines, or might contain a combination of multiple patch and extension baselines.

To create, edit, or delete baselines and baseline groups, you must have the **Manage Baseline** privilege. To attach baselines and baseline groups, you must have the **Attach Baseline** privilege. Privileges must be assigned on the vCenter Server system with which Update Manager is registered. For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see Update Manager Privileges.

This chapter includes the following topics:

- Creating and Managing Baselines
- Creating and Managing Baseline Groups

- Attach Baselines and Baseline Groups to Objects
- Attach Baselines and Baseline Groups to Objects in the vSphere Web Client
- Detach Baselines and Baseline Groups from Objects
- Detach Baselines and Baseline Groups from Objects in the vSphere Web Client

Creating and Managing Baselines

You can create custom patches, extensions, and upgrade baselines to meet the needs of your specific deployment by using the **New Baseline** wizard. You create and manage baselines in the Update Manager Client Administration view.

Update Manager also provides default baselines that you cannot edit or delete. Default baselines are the predefined baselines that contain patches for hosts and updates for VMs. The other type of default baselines is the system managed baselines that you can use to check if your vSAN clusters run the latest supported software.

Create and Edit Patch or Extension Baselines

You can remediate hosts against baselines that contain patches or extensions. Depending on the patch criteria you select, patch baselines can be either dynamic or fixed.

Dynamic patch baselines contain a set of patches, which updates automatically according to patch availability and the criteria that you specify. Fixed baselines contain only patches that you select, regardless of new patch downloads.

Extension baselines contain additional software modules for ESXi hosts. This additional software might be VMware software or third-party software. You can install additional modules by using extension baselines, and update the installed modules by using patch baselines.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, and you have more than one Update Manager instance, patch and extension baselines that you create are not applicable to all inventory objects managed by other vCenter Server systems. Baselines are specific for the Update Manager instance you select.

Prerequisites

Ensure that you have the **Manage Baseline** privilege.

- Create a Fixed Patch Baseline

  Fixed baselines consist of a specific set of patches that do not change as patch availability changes.
- Create a Fixed Patch Baseline in the vSphere Web Client

  Fixed baselines consist of a specific set of patches that do not change as patch availability changes.
- Create a Dynamic Patch Baseline

  Dynamic baselines consist of a set of patches that meet certain criteria. The contents of a dynamic baseline varies as the available patches change. You can also exclude or add specific patches. Patches you select to add or exclude do not change with new patch downloads.

- Create a Dynamic Patch Baseline in the vSphere Web Client

  Dynamic baselines consist of a set of patches that meet certain criteria. The contents of a dynamic baseline varies as the available patches change. You can also exclude or add specific patches. Patches you select to add or exclude do not change with new patch downloads.

- Create a Host Extension Baseline

  Extension baselines contain additional software for ESXi hosts. This additional software might be VMware software or third-party software. You create host extension baselines using the **New Baseline** wizard.

- Create a Host Extension Baseline in the vSphere Web Client

  Extension baselines contain additional software for ESXi hosts. This additional software might be VMware software or third-party software. You create host extension baselines using the **New Baseline** wizard.

- Filter Patches or Extensions in the New Baseline Wizard

  When you create a patch or extension baseline, you can filter the patches and extensions available in the Update Manager repository to find specific patches and extensions to exclude or include in the baseline.

- Edit a Patch Baseline

  You can edit an existing host patch baselines.

- Edit a Patch Baseline in the vSphere Web Client

  You can edit an existing host patch baseline.

- Edit a Host Extension Baseline

  You can change the name, description, and composition of an existing extension baseline.

- Edit a Host Extension Baseline in the vSphere Web Client

  You can change the name, description, and composition of an existing extension baseline.

Create a Fixed Patch Baseline

Fixed baselines consist of a specific set of patches that do not change as patch availability changes.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

  Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

  The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Click **New**, and click **New Baseline**.

The **Baseline Definition** wizard opens.

5 Type a name, and optionally, a description of the baseline.

6 To create an ESXi patch baseline, select **Patch**, and click **Next**.

7 On the **Select Patches Automatically** page, deselect the option to automatically update the baseline with patches that match your criteria, and click **Next**.

You create a fixed patch baseline.

8 On the **Select Patches Manually** page, select the patches that you want to include in the baseline, and click **Next**.

9 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

The new baseline is listed in the **Baselines** tab.

What to do next

Attach the baseline to a data center, a cluster, or a host.

Create a Fixed Patch Baseline in the vSphere Web Client

Fixed baselines consist of a specific set of patches that do not change as patch availability changes.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **Host Baselines** tab, click **New baseline**.

6 Type a name, and optionally, a description of the baseline.

7 Under Baseline Type, select **Host Patch**, and click **Next**.

8 On the Patch Options page, select **Fixed** for the type of baseline, and click **Next**.

9 Select individual patches to include in the baseline.

10 (Optional) Click **Advanced** to find specific patches to include in the baseline.

11 Click **Next**.

12 Review the Ready to Complete page, and click **Finish**.

The new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

Create a Dynamic Patch Baseline

Dynamic baselines consist of a set of patches that meet certain criteria. The contents of a dynamic baseline varies as the available patches change. You can also exclude or add specific patches. Patches you select to add or exclude do not change with new patch downloads.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1. Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2. Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3. Click **Baselines**.
4. Click **New**, and click **New Baseline**.

   The **Baseline Definition** wizard opens.

5. Type a name, and optionally, a description of the baseline.
6. To create an ESXi patch baseline, select **Patch**, and click **Next**.
7. On the **Select Patches Automatically** page, select the option to automatically update the baseline with patches that match your criteria, and click **Next**.

   You create a dynamic patch baseline.

8. Specify the criteria to define the patches to include.

Option	Description
Patch Vendor	Specifies which patch vendor to use.
Product	Restricts the set of patches to the selected products or operating systems. The asterisk at the end of a product name is a wildcard character for any version number.
Severity	Specifies the severity of patches to include.
Category	Specifies the category of patches to include.
Release Date	Specifies the range for the release dates of the patches.

   The relationship between these fields is defined by the Boolean operator AND.

   For example, when you select a product and severity option, the patches are restricted to the ones that are applicable for the selected product and are of the specified severity level.

9 From the **Matched**, **Excluded** and **Selected** tabs in the wizard, you can deselect patches from the ones that matched your criteria, and exclude them permanently from the baseline.

10 Click **Next**.

11 (Optional) On the **Select Patches Manually** page, select individual patches to include in the baseline, and click **Next**.

   The patches that are displayed in this page are patches that do not match the criteria you set in the **Select Patches Automatically** page.

   The patches you add manually to the dynamic baseline stay in the baseline regardless of the automatically downloaded patches that match your criteria.

12 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

The new baseline is listed in the **Baselines** tab.

What to do next

Attach the baseline to a data center, a cluster, or a host.

Create a Dynamic Patch Baseline in the vSphere Web Client

Dynamic baselines consist of a set of patches that meet certain criteria. The contents of a dynamic baseline varies as the available patches change. You can also exclude or add specific patches. Patches you select to add or exclude do not change with new patch downloads.

Prerequisites

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **Host Baselines** tab, click **Create a new baseline**.

6 Type a name, and optionally, a description of the baseline.

7 Under Baseline Type select **Host Patch**, and click **Next**.

8 On the Patch Options page, select **Dynamic** as the type of baseline, and click **Next**.

9 On the Criteria page, specify the criteria to define the patches to include, and then click **Next**.

Option	Description
Patch Vendor	Specifies which patch vendor to use.
Product	Restricts the set of patches to the selected products or operating systems. The asterisk at the end of a product name is a wildcard character for any version number.
Severity	Specifies the severity of patches to include.
Category	Specifies the category of patches to include.
Release Date	Specifies the range for the release dates of the patches.

The relationship between these fields is defined by the Boolean operator AND.

For example, when you select a product and severity option, the patches are restricted to the ones that are applicable for the selected product and are of the specified severity level.

10 (Optional) On the Patches to Exclude page, select one or more patches from the list.

11 (Optional) Click **Advanced** to search for specific patches to exclude from the baseline.

12 Click **Next**.

13 (Optional) On the Additional patches page, select individual patches to include in the baseline and click the down arrow to move them into the Fixed Patches to Add list.

The patches you add to the dynamic baseline stay in the baseline regardless of the new downloaded patches.

14 (Optional) Click **Advanced** to search for specific patches to include in the baseline.

15 Click **Next**.

16 Review the Ready to Complete page, and click **Finish**.

The new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

Create a Host Extension Baseline

Extension baselines contain additional software for ESXi hosts. This additional software might be VMware software or third-party software. You create host extension baselines using the **New Baseline** wizard.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Click **New**, and click **New Baseline**.

   The **Baseline Definition** wizard opens.

5 Type a name, and optionally, a description of the baseline.

6 To create an extension baseline, select **Extension**, and click **Next**.

7 On the Extensions page, select individual extensions to include in the baseline, and click **Next**.

8 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

The new baseline is listed in the **Baselines** tab.

What to do next

Attach the baseline to a data center, a cluster, or a host.

Create a Host Extension Baseline in the vSphere Web Client

Extension baselines contain additional software for ESXi hosts. This additional software might be VMware software or third-party software. You create host extension baselines using the **New Baseline** wizard.

Extensions can provide additional features, updated drivers for hardware, Common Information Model (CIM) providers for managing third-party modules on the host, improvements to the performance or usability of existing host features, and so on.

Host extension baselines that you create are always fixed. You must carefully select the appropriate extensions for the ESXi hosts in your environment.

To perform the initial installation of an extension, you must use an extension baseline. After the extension is installed on the host, you can update the extension module with either patch or extension baselines.

Note When applying extension baselines by using Update Manager, you must be aware of the functional implications of new modules to the host. Extension modules might alter the behavior of ESXi hosts. During installation of extensions, Update Manager only performs the checks and verifications expressed at the package level.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **Host Baselines** tab, click **New baseline**.

6 Type a name, and optionally, a description of the baseline.

7 Under Baseline Type, select **Host Extension**, and click **Next**.

8 On the Extensions page, select individual extensions to include in the baseline.

9 (Optional) Select an extension, and click **Show Patch Details** to see additional information.

10 Click **Next**.

11 Review the Ready to Complete page, and click **Finish**.

The new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

Filter Patches or Extensions in the New Baseline Wizard

When you create a patch or extension baseline, you can filter the patches and extensions available in the Update Manager repository to find specific patches and extensions to exclude or include in the baseline.

Procedure

1 In the **New Baseline** wizard, click **Advanced**.

- If you are creating a fixed patch baseline, on the Patches page, click **Advanced**.
- If you are creating a dynamic patch baseline, on the Patches to Exclude or Additional Patches page, click **Advanced**.
- If you are creating a host extension baseline, on the Extensions page, click **Advanced**.

2 On the Filter Patches or Filter Extensions page, specify the criteria to define the patches or extensions to include or exclude.

Option	Description
Patch Vendor	Specifies which patch or extension vendor to use.
Product	Restricts the set of patches or extensions to the selected products or operating systems. The asterisk at the end of a product name is a wildcard character for any version number.
Severity	Specifies the severity of patches or extensions to include.
Category	Specifies the category of patches or extensions to include.
Release Date	Specifies the range for the release dates of the patches or extensions.
Text	Restricts the patches or extensions to those containing the text that you enter.

The relationship between these fields is defined by the Boolean operator AND.

3 Click **Find**.

The patches or extensions in the **New Baseline** wizard are filtered with the criteria that you specified.

Edit a Patch Baseline

You can edit an existing host patch baselines.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Select a baseline from the list, and click **Edit**.

The **Baseline Definition** wizard opens.

5 Edit the name, and optionally, the description of the baseline.

6 (Optional) Change the criteria for patch selection, and click **Next**.

7 (Optional) Change the selected patches, and click **Next**.

You can deselect patches, or select new ones to include in the patch baseline.

8 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

What to do next

Attach the baseline to a data center, a cluster, or a host.

Edit a Patch Baseline in the vSphere Web Client

You can edit an existing host patch baseline.

In the vSphere Web Client, you edit patch baselines from the Update Manager Admin view.

Prerequisites

Ensure that you have the **Manage Baseline** privilege.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 Click **Host Baselines**.

6 Select a patch baseline and click **Edit** above the Baselines pane.

7 Edit the name and description of the baseline and click **Next**.

8 Go through the **Edit Baseline** wizard to change the criteria, and select patches to include or exclude.

9 Review the Ready to Complete page, and click **Finish**.

Edit a Host Extension Baseline

You can change the name, description, and composition of an existing extension baseline.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Select a baseline from the list, and click **Edit**.

   The **Baseline Definition** wizard opens.

5 Edit the name, and optionally, the description of the baseline.

6 (Optional) Change the included extensions, and click **Next**.

7 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

What to do next

Attach the baseline to a data center, a cluster, or a host.

Edit a Host Extension Baseline in the vSphere Web Client

You can change the name, description, and composition of an existing extension baseline.

In the vSphere Web Client, you edit patch baselines from the Update Manager Admin view.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines.Manage Baseline**.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 Click **Host Baselines** .

6 Select an extension baseline, and click **Edit** above the Baselines pane.

7 Edit the name and description of the baseline, and click **Next**.

8 Make your changes by going through the **Edit Baseline** wizard.

9 Review the Ready to Complete page, and click **Finish**.

Create and Edit Host Upgrade Baselines

You can create an ESXi host upgrade baseline by using the **New Baseline** wizard. You can create host baselines with already uploaded ESXi 6.5 images.

You can upload and manage ESXi images from the **ESXi Images** tab of the Update Manager Administration view.

Update Manager 6.7 supports upgrade from ESXi 6.0.x and ESXi 6.5.x to ESXi 6.7.

Before uploading ESXi images, obtain the image files from the VMware Web site or another source. You can create custom ESXi images that contain third-party VIBs by using vSphere ESXi Image Builder. For more information, see *Customizing Installations with vSphere ESXi Image Builder*.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, and you have more than one Update Manager instance, host upgrade files that you upload and baselines that you create are not applicable to the hosts managed by other vCenter Server systems. Upgrade files and baselines are specific for the Update Manager instance you select.

- Import ESXi Host Upgrade Images

  Import ESXi images to create upgrade baselines, which you can use to upgrade the host in your vSphere inventory.

- Create a Host Upgrade Baseline

  You can create upgrade baselines for ESXi hosts with ESXi 6.7 images that you import to the Update Manager repository.

- Import Host Upgrade Images and Create Host Upgrade Baselines in the vSphere Web Client

  You can create upgrade baselines for ESXi hosts with ESXi 6.5 images that you import to the Update Manager repository.
- Create a Host Upgrade Baseline in the vSphere Web Client

  To upgrade the hosts in your vSphere environment, you must create host upgrade baselines.
- Edit a Host Upgrade Baseline

  You can change the name and type of an existing baseline group. You can also edit a baseline group by adding or removing the upgrade and patch baselines. You cannot add system managed baselines to a custom baseline group.
- Edit a Host Upgrade Baseline in the vSphere Web Client

  You can change the name, description, and upgrade options of an existing host upgrade baseline. You cannot delete a host upgrade image by editing the host upgrade baseline.
- Delete ESXi Images

  You can delete ESXi images if you no longer need them.
- Delete ESXi Images in the vSphere Web Client

  You can delete ESXi images from the Update Manager repository if you no longer need them.

Import ESXi Host Upgrade Images

Import ESXi images to create upgrade baselines, which you can use to upgrade the host in your vSphere inventory.

- Required privileges: **VMware vSphere Update Manager.Upload File**.

You can use ESXi `.iso` images to upgrade ESXi 6.0.x hosts and ESXi 6.5.x hosts to ESXi 6.7.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-6.7.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

  Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

  The Update Manager administrative home view opens.

3 Click **ESXi Images**, and click **Import**.

  The **Import ESXi Image** wizard opens.

4 Click **Browse** to navigate and select an ESXi image that you want to upload, or type a URL address to the ESXi image.

Note You can import ESXi `.iso` images of version 6.7.

5 Wait for the upload progress of the ESXi image to complete, and click **Import**.

The ESXi image that you uploaded, appears in the list of ESXi images. You can review information about the ESXi image such as product and version details, vendor, acceptance level, and creation date of the image.

What to do next

Attach the baseline group to a data center, a cluster, or a host.

Create a Host Upgrade Baseline

You can create upgrade baselines for ESXi hosts with ESXi 6.7 images that you import to the Update Manager repository.

You can use ESXi `.iso` images to upgrade ESXi 6.0.x hosts and ESXi 6.5.x hosts to ESXi 6.7.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-6.7.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.
- Verify that you have an ESXi 6.7 uploaded to Update Manager. For more information, see Import ESXi Host Upgrade Images.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Click **New**, and click **New Baseline**.

The **Baseline Definition** wizard opens.

5 Type a name, and optionally, a description of the baseline.

6 To create an ESXi upgrade baseline, select **Upgrade**, and click **Next**.

7 On the **Select Image** page, select an ESXi image, and click **Next**.

8 Click **Next**.

9 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

The new baseline is listed in the **Baselines** tab.

What to do next

Attach the baseline to a data center, a cluster, or a host.

Import Host Upgrade Images and Create Host Upgrade Baselines in the vSphere Web Client

You can create upgrade baselines for ESXi hosts with ESXi 6.5 images that you import to the Update Manager repository.

You can use ESXi `.iso` images to upgrade ESXi 6.0.x hosts and ESXi 6.5.x hosts to ESXi 6.7.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-6.7.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Upload File**.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 Click **ESXi Images**, and click **Import ESXi Image**.

6 On the Select ESXi Image page of the **Import ESXi Image** wizard, browse to and select the ESXi image that you want to upload.

7 Click **Next**.

   Caution Do not close the import wizard. Closing the import wizard stops the upload process.

8 (Optional) In the **Security Warning** window, select an option to handle the certificate warning.

A trusted certificate authority does not sign the certificates that are generated for vCenter Server and ESXi hosts during installation. Because of this, each time an SSL connection is made to one of these systems, the client displays a warning.

Option	Action
Ignore	Click **Ignore** to continue using the current SSL certificate and start the upload process.
Cancel	Click **Cancel** to close the window and stop the upload process.
Install this certificate and do not display any security warnings	Select this check box and click **Ignore** to install the certificate and stop receiving security warnings.

9 After the file is uploaded, click **Next**.

10 (Optional) Create a host upgrade baseline.

a Leave the **Create a baseline using the ESXi image** selected.

b Specify a name, and optionally, a description for the host upgrade baseline.

11 Click **Finish**.

The ESXi image that you uploaded appears in the Imported ESXi Images pane. You can see more information about the software packages that are included in the ESXi image in the Software Packages pane.

If you also created a host upgrade baseline, the new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

What to do next

To upgrade the hosts in your environment, you must create a host upgrade baseline if you have not already done so.

Create a Host Upgrade Baseline in the vSphere Web Client

To upgrade the hosts in your vSphere environment, you must create host upgrade baselines.

Prerequisites

Upload at least one ESXi image.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **Host Baselines** tab, click **New baseline**.

6 Type a name, and optionally, a description of the baseline.

7 Under Baseline Type, select **Host Upgrade**, and click **Next**.

8 On the ESXi Image page, select a host upgrade image and click **Next**.

9 Review the Ready to Complete page and click **Finish**.

The new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

Edit a Host Upgrade Baseline

You can change the name and type of an existing baseline group. You can also edit a baseline group by adding or removing the upgrade and patch baselines. You cannot add system managed baselines to a custom baseline group.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

> **Note** In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Select a baseline from the list, and click **Edit**.

The **Baseline Definition** wizard opens.

5 Edit the name, and optionally, the description of the baseline.

6 (Optional) Change the included ESXi image, and click **Next**.

7 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

What to do next

Attach the baseline to a data center, a cluster, or a host.

Edit a Host Upgrade Baseline in the vSphere Web Client

You can change the name, description, and upgrade options of an existing host upgrade baseline. You cannot delete a host upgrade image by editing the host upgrade baseline.

In the vSphere Web Client you can edit upgrade baselines from the Update Manager Client Administration view.

Prerequisites

Ensure that you have the **Manage Baseline** privilege.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 Click **Host Baselines** .

6 Select an existing host upgrade baseline, and click **Edit** above the Baselines pane.

7 Edit the name and description of the baseline, and click **Next**.

8 Make your changes by going through the **Edit Baseline** wizard.

9 Review the Ready to Complete page, and click **Finish**.

Delete ESXi Images

You can delete ESXi images if you no longer need them.

Prerequisites

- Verify that the ESXi images you want to delete are not part of any baselines. You cannot delete images that are included in a baseline.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3 Click **ESXi Images**.

4 Select an ESXi image from the list, and click **Delete**.

Note Deleting an ESXi image that is used in a baseline fails with an error message. To delete a ESXi image that is part of a baseline, first delete the baseline.

5 Click **Yes** to confirm the deletion.

The ESXi image is deleted and no longer available.

Delete ESXi Images in the vSphere Web Client

You can delete ESXi images from the Update Manager repository if you no longer need them.

Connect thevSphere Web Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** icon.

Prerequisites

Verify that the ESXi images are not included in baselines. You cannot delete images that are included in a baseline.

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab.

4 Click the **ESXi Images** tab.

5 Under Imported ESXi Images, select the file you want to delete and click **Delete**.

6 Click **Yes** to confirm the deletion.

The ESXi image is deleted and no longer available.

Delete Baselines

You can delete baselines that you no longer need to use with Update Manager. Deleting a baseline detaches it from all the objects to which the baseline is attached. You cannot delete predefines and system-managed baselines.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Select a baseline from the list, and click **Delete**.

You cannot delete predefined baselines and system managed baselines.

5 Confirm the deletion.

Delete Baselines in the vSphere Web Client

You can delete baselines that you no longer need from Update Manager. Deleting a baseline detaches it from all the objects to which the baseline is attached.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **VMs Baselines** tab, select the baselines to remove, and click **Delete the baseline definition**.

6 In the confirmation dialog box, click **Yes**.

The baseline is deleted.

Creating and Managing Baseline Groups

A baseline group consists of a set of non-conflicting baselines. Baseline groups allow you to scan and remediate objects against multiple baselines at the same time.

You can perform an orchestrated upgrade of the virtual machines by remediating the same folder or datacenter against a baseline group containing the following baselines:

- VMware Tools Upgrade to Match Host
- VM Hardware Upgrade to Match Host

You can perform an orchestrated upgrade of hosts by using a baseline group that contains a single host upgrade baseline and multiple patch or extension baselines.

You can create two types of baseline groups depending on the object type to which you want to apply them:

- Baseline groups for hosts
- Baseline groups for virtual machines

Baseline groups that you create are displayed on the **Baselines and Groups** tab of the Update Manager Client Administration view.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, and you have more than one Update Manager instance, baseline groups you create are not applicable to all inventory objects managed by other vCenter Server systems in the group. Baseline groups are specific for the Update Manager instance that you select.

Create a Host Baseline Group

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group. You cannot add system managed baselines to a custom baseline group.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Click **New**, and click **New Baseline Group**.

   The **Baseline Group Definition** wizard opens.

5 Type a unique name, and optionally, a description of the baseline group.

6 Click **Next**.

7 Select a host upgrade baseline to include it in the baseline group, and click **Next**.

8 Select the patch baselines that you want to include in the baseline group, and click **Next**.

9 Select the extension baselines to include in the baseline group, and click **Next**.

10 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

The host baseline group is displayed in the **Baselines and Baseline Groups** pane.

What to do next

Attach the baseline group to a data center, a cluster, or a host.

Create a Host Baseline Group in the vSphere Web Client

You can combine one host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group.

Note You can click **Finish** in the **New Baseline Group** wizard at any time to save your baseline group and add baselines to it at a later stage.

Procedure

1. Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.
2. In the Home view of the vSphere Web Client, select the Update Manager icon.
3. From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
4. Click the **Manage** tab.
5. On the **Host Baselines** tab, click **New Baseline Group** above the Baseline Groups pane.
6. Enter a unique name for the baseline group and click **Next**.
7. Select a host upgrade baseline to include it in the baseline group.
8. (Optional) Create a new host upgrade baseline by clicking **Create a new Host Upgrade Baseline** at the bottom of the Upgrades page, and complete the **New Baseline** wizard.
9. Click **Next**.
10. Select the patch baselines that you want to include in the baseline group.
11. (Optional) Create a new patch baseline by clicking **Create a new Host Patch Baseline** at the bottom of the Patches page, and complete the **New Baseline** wizard.
12. Click **Next**.
13. Select the extension baselines to include in the baseline group.
14. (Optional) Create a new extension baseline by clicking **Create a new Extension Baseline** at the bottom of the Patches page, and complete the **New Baseline** wizard.
15. Review the Ready to Complete page, and click **Finish.**

The host baseline group is displayed in the Baseline Groups pane.

Create a Virtual Machine Baseline Group

You can combine upgrade baselines in a virtual machine baseline group.

Note You can click **Finish** in the **New Baseline Group** wizard at any time to save your baseline group, and add baselines to it at a later stage.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **Baselines** tab, click **Create new baseline definition group**.

6 Enter a name for the baseline group, and click **Next**.

7 For each type of upgrade (virtual hardware and VMware Tools), select one of the available upgrade baselines to include in the baseline group.

8 Click **Next**.

9 Review the Ready to Complete page, and click **Finish**.

The new baseline group is displayed in the Baseline Groups pane.

Edit a Baseline Group

You can change the name and type of an existing baseline group. You can also edit a baseline group by adding or removing the upgrade and patch baselines. You cannot add system managed baselines to a custom baseline group.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Select a baseline group from the list, and click **Edit**.

   The **Baseline Group Definition** wizard opens.

5 Edit the name, and optionally, the description of the baseline group.

6 Select a host upgrade baseline to include it in the baseline group, and click **Next**.

7 (Optional) Change the included patch baselines (if any), and click **Next**.

8 (Optional) Change the included extension baselines (if any), and click **Next**.

9 On the **Ready to Complete** page, review the selections you made, and click **Finish**.

What to do next

Attach the baseline group to a data center, a cluster, or a host.

Edit a Baseline Group in the vSphere Web Client

You can change the name and type of an existing baseline group. You can also edit a baseline group by adding or removing the upgrade and patch baselines a baseline group contains.

In the vSphere Web Client, you edit baseline groups from the Update Manager Admin view.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines.Manage Baseline**.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 Click **VMs Baselines** .

6 Select an existing baseline, and click **Edit existing baseline definition**.

7 Edit the name of the baseline group.

8 (Optional) Change the included upgrade baselines (if any).

9 (Optional) Change the included patch baselines (if any).

10 (Optional) Change the included extension baselines (if any).

11 Review the Ready to Complete page and click **OK**.

Add Baselines to a Baseline Group

You can add a patch, extension, or upgrade baseline to an existing baseline group.

In the vSphere Web Client, you can add baselines to baseline groups from the Update Manager Administration view.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines.Manage Baseline**.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **VMs Baselines** tab, select an existing baseline group, and click **Edit existing baseline group definition**.

6 From the Upgrades page, select a baseline group and expand it to view the included baselines.

7 Select or deselect the baselines from the list.

The baseline is added to the selected baseline group.

Remove Baselines from a Baseline Group

You can remove individual baselines from existing baseline groups.

In the vSphere Web Client, you can edit the contents of baseline groups from the Update Manager Admin view.

Prerequisites

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **VMs Baselines** tab, select an existing baseline group, and expand it to view the included baselines.

6 Select a baseline from the Baseline Groups pane on the right and click the left arrow.

The baseline is removed from the selected baseline group.

Delete Baseline Groups

You can delete baseline groups that you no longer need to use with Update Manager.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3 Click **Baselines**.

4 Select a baseline group from the list, and click **Delete**.

5 Confirm the deletion.

The baseline group is detached from any inventory objects and deleted.

Delete Baseline Groups in the vSphere Web Client

You can delete baseline groups that you no longer need from Update Manager. Deleting a baseline group detaches it from all the objects to which the baseline group is attached.

In the vSphere Web Client, you can delete baseline groups from the Update Manager Admin view.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the Home view of the vSphere Web Client, select the Update Manager icon.

3 From the **Objects** tab, select an Update Manager instance.

The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

4 Click the **Manage** tab.

5 On the **VMs Baselines** tab, select an existing baseline group, and click **Delete**.

6 In the confirmation dialog box, click **Yes**.

The baseline group is deleted.

Attach Baselines and Baseline Groups to Objects

To view compliance information and scan objects in the inventory against baselines and baseline groups, you must first attach existing baselines and baseline groups to the objects.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines.Attach Baseline**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Select **Menu > Hosts and Clusters**, and select a host or a cluster from the vSphere inventory.

3 Select the **Updates** tab.

You are in the Update Manager compliance view.

4 Select an object or a container object from the inventory, and click **Attach**.

The **Attach Baselines** dialog box opens.

5 In the **Attach Baseline or Baseline Group** dialog box, select one or more baselines or baseline groups to attach to the object.

If you select one or more baseline groups, all baselines in the groups are selected. You cannot deselect individual baselines in a group.

6 Click **OK**.

What to do next

Scan the selected object against the attached baselines.

Attach Baselines and Baseline Groups to Objects in the vSphere Web Client

To view compliance information and scan objects in the inventory against baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects. You can attach baselines and baseline groups to objects.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines.Attach Baseline**.

Procedure

1. Select the type of object in the vSphere Web Client object navigator.

   For example, **Hosts and Clusters** or **VMs and Templates**, and select an object or a container object.

2. Select the **Update Manager** tab.
3. In the **Attach Baseline or Baseline Group** window, select one or more baselines or baseline groups to attach to the object.

   If you select one or more baseline groups, all baselines in the groups are selected. You cannot deselect individual baselines in a group.

4. (Optional) Create a baseline or a baseline group, if the existing baselines and groups do not match your task, and complete the remaining steps in the respective wizard.

   The **Attach Baseline or Group** window collapses to the Work In Progress pane, and the respective **New Baseline Group** window or **New Baseline Group** window opens. When you complete the steps to create the baseline or the baseline group, the **Attach Baseline or Group** window reopens.

5. Click **OK**.

What to do next

Scan the selected object against the attached baselines.

Detach Baselines and Baseline Groups from Objects

You can detach baselines and baseline groups from objects. Because vSphere inventory objects can have inherited properties, you might have to select the container object where the baseline or the baseline group is attached in order to detach it from a lower-level object.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines.Attach Baseline**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Select **Menu > Hosts and Clusters**, and select a host or a cluster from the vSphere inventory.

3 Select the **Updates** tab.

   You are in the Update Manager compliance view.

4 Select an object or a container object from the inventory.

5 Select a baseline or a baseline group from the list, and click **Detach**.

   The **Detach Baselines** dialog box opens.

6 In the **Detach Baseline Group** dialog box, select the entities that you want to detach the baseline or the baseline group from.

7 Click **OK**.

The baseline or baseline group that you detach is no longer listed in the Attached Baselines and Baseline Groups list on the **Updates** tab.

Detach Baselines and Baseline Groups from Objects in the vSphere Web Client

You can detach baselines and baseline groups from objects to which the baselines or baseline groups are directly attached. Because vSphere objects can have inherited properties, you might have to select the container object where the baseline or baseline group is attached and then detach it from the container object.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Baselines.Attach Baseline**.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 In the vSphere Web Client navigator, select **Hosts and Clusters** or **VMs and Templates**.

3 Select the object in the inventory, and select **Update Manager**.

4 Remove a baseline or a baseline group that is attached to the object.

   a To remove a baseline, select the baseline, and click **Detach** on the upper left corner of the Attached Baselines pane.

   b To remove a baseline group, select the baseline group from the **Attached Baseline Groups** drop-down menu, and click **Detach** at the upper right corner of the **Attached Baseline Groups** drop-down menu.

      You cannot detach an individual baseline from the group. You can only detach the entire baseline group.

5 In the Detach Baseline Group dialog box, select the entities that you want to detach the baseline or the baseline group from.

6 Click **OK**.

The baseline or baseline group that you detach is no longer listed in the Attached Baselines pane or the Attached Baseline Groups drop-down menu.

Scanning vSphere Objects and Viewing Scan Results

8

Scanning is the process in which attributes of a set of hosts and virtual machines are evaluated against the patches, extensions, and upgrades included in the attached baselines and baseline groups.

You can configure Update Manager to scan virtual machines and ESXi hosts by manually initiating or scheduling scans to generate compliance information. To generate compliance information and view scan results, you must attach baselines and baseline groups to the objects you scan.

To initiate or schedule scans, you must have the **Scan for Applicable Patches, Extensions, and Upgrades** privilege. For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see Update Manager Privileges.

You can scan vSphere objects from the Update Manager Client Compliance view.

This chapter includes the following topics:

- Manually Initiate a Scan of ESXi Hosts
- Manually Initiate a Scan of Virtual Machines
- Manually Initiate a Scan of a Container Object
- Schedule a Scan
- Viewing Scan Results and Compliance States for vSphere Objects

Manually Initiate a Scan of ESXi Hosts

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 Select **Home > Hosts and Clusters**.

3 Select a host.

4 Select the **Update Manager** tab.

5 Click **Scan for Updates**.

   The Scan for Updates dialog box opens.

6 Select the types of updates to scan for.

   You can scan for **Patches and Extensions** and **Upgrades**.

7 Click **OK**.

The selected host, or the container object is scanned against all patches, extensions, and upgrades in the attached baselines.

What to do next

Stage and remediate the scanned inventory object with Update Manager in the vSphere Web Client.

Manually Initiate a Scan of Virtual Machines

You can scan virtual machines in the vSphere inventory against attached baselines and baseline groups.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 From the inventory object navigator, select a virtual machine, and click the **Update Manager** tab.

3 Click **Scan for Updates**.

   The Scan for Updates wizard opens.

4 Select the types of updates to scan for.

   You can scan for **VMware Tools upgrades**, and **VM Hardware upgrades**.

5 Click **OK**.

The virtual machines are scanned against the attached baselines, depending on the options that you selected.

What to do next

Stage and remediate the scanned inventory object with Update Manager in the vSphere Web Client.

Manually Initiate a Scan of a Container Object

Start a simultaneous scan of hosts and virtual machines by scanning a container object that is a data center or a data center folder.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 From the inventory object navigator, right-click a vCenter Server instance, a data center, a cluster, or a VM Folder, and select **Update Manager > Scan for Updates**.

   The Scan wizard opens.

3 Select the types of updates for which you want to perform scan operation.

   - For the ESXi hosts in the container object, you can scan for **Patches and Extensions** and **Upgrades**.
   - For virtual machines in the data center, you can scan for **VMware Tools upgrades**, and **VM Hardware upgrades**.

4 Click **OK**.

The selected inventory object and all child objects are scanned against the attached baselines, depending on the options that you selected. The larger the virtual infrastructure and the higher up in the object hierarchy you initiate the scan, the longer the scan takes.

What to do next

Stage and remediate the scanned inventory object with Update Manager in the vSphere Web Client.

Schedule a Scan

You can configure the vSphere Web Client to scan virtual machines and ESXi hosts at specific times or at intervals that are convenient for you.

Procedure

1 Connect the vSphere Web Client to a vCenter Server system with which Update Manager is registered, and select an object from the inventory.

   If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, specify the Update Manager instance that you want to use to schedule a scan task by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 In the inventory tree, select the inventory object to be scanned.

   All child objects of the object that you select are also scanned.

3 Select the **Monitor** tab, and click **Task & Events**.

4 Select **Scheduled Tasks**, and click **Schedule a New Task**.

5 Select **Scan for Updates** from the drop-down list that appears.

   The Scan for Updates wizard opens.

6 On the Edit Settings page, select the types of updates to scan the inventory object for.

   You must select at least one scan type.

7 On the Scheduling options page, describe and schedule the scan task.

   a Enter a unique name, and optionally, a description for the scan task.

   b Click **Change** to set the frequency and the start time for the scan task.

   c (Optional) Specify one or more email addresses to receive notification after the scan task is complete.

      You must configure mail settings for the vCenter Server system to enable this option.

8 Click **OK**.

The scan task is listed in the **Scheduled Tasks** view of the vSphere Web Client.

Viewing Scan Results and Compliance States for vSphere Objects

Update Manager scans objects to determine how they comply with the attached baselines and baseline groups. You can review compliance by examining results for a single virtual machine, template, or ESXi host, as well as for a group of virtual machines or hosts.

Supported groups of virtual machines or ESXi hosts include virtual infrastructure container objects such as folders, vApps, clusters, and datacenters.

Baselines and baseline groups interact with virtual machines, templates, and hosts in the following ways:

- Objects must have an attached baseline or baseline group to be examined for compliance information.
- Compliance with baselines and baseline groups is assessed at the time of viewing, so a brief pause might occur while information is gathered to make sure that all information is current.
- Compliance status is displayed based on privileges. Users with the privilege to view a container, but not all the contents of the container are shown the aggregate compliance of all objects in the container. If a user does not have permission to view an object, its contents, or a particular virtual machine, the results of those scans are not displayed. To view the compliance status, the user must also have the privilege to view compliance status for an object in the inventory. Users that have privileges to remediate against patches, extensions, and upgrades and to stage patches and extensions on a particular inventory object, can view the compliance status of the same object even if they do not have the view compliance privilege. For more information about the Update Manager privileges, see Update Manager Privileges. For more information about managing users, groups, roles and permissions, see *vCenter Server and Host Management*.

In the vSphere infrastructure hierarchy, the baseline and baseline groups you attach to container objects are also attached to the child objects. Consequently, the computed compliance state is also inherited. For example, a baseline or baseline group attached to a folder is inherited by all objects in the folder (including subfolders), but the status of inherited baselines or baseline groups propagates upwards, from the contained objects to the folder. Consider a folder that contains two objects A and B. If you attach a

baseline (baseline 1) to the folder, both A and B inherit baseline 1. If the baseline state is noncompliant for A and compliant for B, the overall state of baseline 1 against the folder is non-compliant. If you attach another baseline (baseline 2) to B, and baseline 2 is incompatible with B, the overall status of the folder is incompatible.

Note After a download of patch recall notifications, Update Manager flags recalled patches but their compliance state does not refresh automatically. You must perform a scan to view the updated compliance state of patches affected by the recall.

Check Compliance of a vSphere Inventory Object

Update Manager performs compliance check on the vSphere inventory against the attached baselines on regular basis but you can also manually initiate a compliance check.

Prerequisites

- **VMware vSphere Update Manager.Manage Patches and Upgrades.View Compliance Status**

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Select an object or a container object from the inventory.

3 Select a host or a container object from the inventory.

4 Select the **Updates** tab.

   You are in the Update Manager compliance view.

5 Click **Check Compliance**.

   You can see information about the last time that Update Manager ran a compliance check on the selected hosts against the attached baselines and baseline groups.

Review the refreshed information. If you are viewing information for a single host, Update Manager displays the following information:

- The number of non-compliant baselines that are attached to the host.
- The number of patches that might be missing from the host.
- The number of critical patches that might be missing from the host.

If you are viewing information for a container object, Update Manager displays the following information:

- Information about the hosts that require attention.
- The number of hosts that have non-compliant software.

For a more detailed information, review the compliance information of each individual baseline or baseline group in the **Attached Baselines and Baseline Groups** list.

What to do next

Perform a pre-check remediation of the object.

View Compliance Information for vSphere Objects in the vSphere Web Client

You can review compliance information for the virtual machines and hosts against baselines and baseline groups that you attach.

When you select a container object, you view the overall compliance status of the attached baselines, and all the individual compliance statuses. If you select an individual baseline attached to the container object, you see the compliance status of the baseline.

If you select an individual virtual machine or host, you see the overall compliance status of the selected object against all attached baselines and the number of updates. If you further select an individual baseline attached to this object, you see the number of updates grouped by the compliance status for that baseline.

Procedure

1 Depending on the compliance information you want to see, perform the following steps:

   a To view host compliance information, select **Home > Hosts and Clusters**, and select a host, a cluster, a data center, or a vCenter Server instance.

   b To view virtual machine compliance information, select **Home > VMs and Templates**, and select a virtual machine or a folder.

2 Click the **Update Manager** tab.

3 Select one of the attached baselines to view compliance information for the object against the selected baseline.

You can see the compliance information in the table below the attached baselines to the object.

Review Compliance with Individual vSphere Objects

Scan results provide information about the degree of compliance with attached baselines and baseline groups. You can view information about individual vSphere objects and about the patches, extensions, and upgrades included in a baseline or a baseline group.

The following information is included in the scan results:

- The last time that a scan was completed at this level.
- The total number of noncompliant, incompatible, unknown, and compliant updates.
- For each baseline or baseline group, the number of virtual machines or hosts that are applicable, noncompliant, incompatible, unknown, or compliant.
- For each baseline or baseline group, the number of updates that are applicable to particular virtual machines or hosts.

Procedure

1 Connect the vSphere Web Client to a vCenter Server system with which Update Manager is registered, and select **Home > Inventory**.

2 Select the type of object for which you want to view scan results.

   For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select an individual object from the inventory, such as a virtual machine or host.

4 Click the **Update Manager** tab.

5 Select a baseline group or baseline.

   Select **All Groups and Independent Baselines** in the Attached Baseline Groups pane and **All** in the Attached Baselines pane to view the overall compliance of all attached baselines and baseline groups.

6 In the Compliance pane, select the **All Applicable** compliance status to view the overall compliance status of the selected object.

   The selected object together with the number of patches, upgrades, and extensions (if the selected object is a host) appear in the bottom pane of the **Update Manager** tab.

7 Click a number link in the bottom pane of the Update Manager tab to see more details about updates.

Column	Description
Patches	The link indicates the number of patches in the selected compliance state and opens the **Patch Details** window.
Upgrades	The link indicates the number of upgrades in the selected compliance state and opens the **Upgrade Details** window.
Extensions	The link indicates the number of extensions in the selected compliance state and opens the **Extension Details** window.

Compliance View

Information about the compliance states of selected vSphere inventory objects against baselines and baseline groups you attach is displayed in the Update Manager Client Compliance view.

The information is displayed in four panes.

Table 8-1. Update Manager Tab Panes

Pane	Description
Attached Baseline Groups	Displays the baseline groups attached to the selected object. If you select **All Groups and Independent Baselines**, all attached baselines in the Attached Baselines pane are displayed. If you select an individual baseline group, only the baselines in that group are displayed in the Attached Baselines pane.
Attached Baselines	Displays the baselines attached to the selected object and included in the selected baseline group.

Table 8-1. Update Manager Tab Panes (Continued)

Pane	Description
Compliance	Contains a compliance graph that changes dynamically depending on the inventory object, baseline groups, and baselines that you select. The graph represents the percentage distribution of the virtual machines or hosts in a selected container object that are in a particular compliance state against selected baselines. If you select an individual host or virtual machine, the color of the graph is solid and represents a single compliance state. Above the graph, the following compliance states are displayed: **All Applicable** Total number of inventory objects for which compliance is being calculated. This number is the total of objects in the selected container inventory object minus the objects for which the selected baselines are not applicable. The applicability of a baseline is determined on the basis of whether the baseline is directly attached to the virtual machine or host, or whether it is attached to a container object. Applicability also depends on whether the baseline contains patches, extensions, or upgrades that can be applied to the selected object. **Non-Compliant** Number of virtual machines or hosts in the selected container object that are not compliant with at least one patch, extension, or upgrade in the selected baselines or baseline groups. **Incompatible** Number of virtual machines or hosts in the selected container object that cannot be remediated against the selected baselines and baseline groups. Incompatible state requires more attention and investigation for determining the reason for incompatibility. To obtain more information about the incompatibility, view patch, extension, or upgrade details. **Unknown** Number of virtual machines or hosts in the selected container object that are not scanned against at least one of the patches, extensions, or upgrades in the selected baselines and baseline groups. **Compliant** Number of compliant virtual machines or hosts in the selected container object.
Bottom pane	The information in this pane depends on whether you select an individual object or a container object. If you select a container object, the bottom pane of the **Update Manager** tab displays the following information: - A list of virtual machines or hosts that meet the selections from the Attached Baseline Groups, Attached Baselines and Compliance panes. - The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups.

Table 8-1. Update Manager Tab Panes (Continued)

Pane	Description
	If you select an individual object (such as virtual machine or host), the bottom pane of the **Update Manager** tab displays the following information: ■ The number of patches, extensions, or upgrades included in the baseline or baseline group that you select. ■ The number of staged patches or extensions to a host. ■ The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups.

Compliance States for Updates

In Update Manager, update stands for all patches, extensions, and upgrades that you can apply with Update Manager. The compliance state of the updates in baselines and baseline groups that you attach to objects in your inventory is calculated after you perform a scan of the target object.

Conflict
The update conflicts with either an existing update on the host or another update in the Update Manager patch repository. Update Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform scan, remediation, and staging operations. In most cases, you can take action to resolve the conflict.

Conflicting New Module
The host update is a new module that provides software for the first time, but is in conflict with either an existing update on the host or another update in the Update Manager repository. Update Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform scan, remediation, and staging operations. In most cases, you must take action to resolve the conflict.

Incompatible Hardware
The hardware of the selected object is incompatible or has insufficient resources to support the update. For example, when you perform a host upgrade scan against a 32-bit host or if a host has insufficient RAM.

Installed
Installed compliance state indicates that the update is installed on the target object, and no further user action is required.

Missing
Missing compliance state indicates that the update is applicable to the target object, but not yet installed. You must perform a remediation on the target object with this update, so that the update becomes compliant.

Missing Package This state occurs when metadata for the update is in the depot but the corresponding binary payload is missing. The reasons can be that the product might not have an update for a given locale; the Update Manager patch repository is deleted or corrupt, and Update Manager no longer has Internet access to download updates; or you have manually deleted an upgrade package from the Update Manager repository.

New Module New module compliance state indicates that the update is a new module. An update in this compliance state cannot be installed when it is part of a host patch baseline. When it is part of a host extension baseline, the new module state signifies that the module is missing on the host and can be provisioned by remediation. The compliance state of the baseline depends on the type of baseline containing the update in new module state. If the baseline is a host patch baseline, the overall status of the baseline is compliant. If the baseline is a host extension baseline, the overall status of the baseline is not compliant.

Not Applicable Not applicable compliance state indicates that the patch is not applicable to the target object. A patch might be in not applicable compliance state for one of the following reasons:

- There are other patches in the Update Manager patch repository that obsolete this patch.
- The update does not apply to the target object.

Not Installable The update cannot be installed. The scan operation might succeed on the target object, but remediation cannot be performed.

Obsoleted By Host This compliance state applies mainly to patches. The target object has a newer version of the patch. For example, if a patch has multiple versions, after you apply the latest version to the host, the earlier versions of the patch are in Obsoleted By Host compliance state.

Staged This compliance state applies to host patches and host extensions. It indicates that the update is copied from the Update Manager repository to the host, but is not yet installed. Staged compliance state might occur only when you scan hosts running ESXi 6.0 and later.

Unknown A patch is in unknown state for a target object until Update Manager successfully scans the object. A scan might not succeed if the target object is of an unsupported version, if Update Manager lacks metadata, or if the patch metadata is corrupt.

Unsupported Upgrade The upgrade path is not possible. For example, the current hardware version of the virtual machine is greater than the highest version supported on the host.

Baseline and Baseline Group Compliance States

Compliance states are computed after you scan the objects in your inventory against attached baselines or baseline groups. Update Manager computes the compliance state based on the applicability of the patches, extensions, and upgrades contained in the attached baselines or baseline groups.

Compliant

Compliant state indicates that a vSphere object is compliant with all baselines in an attached baseline group or with all patches, extensions, and upgrades in an attached baseline. Compliant state requires no further action. If a baseline contains patches or upgrades that are not relevant to the target object, the individual updates, and baselines or baseline groups that contain them, are treated as not applicable, and represented as compliant. Compliant are also hosts with attached patch baselines containing extensions or patches in Obsoleted By Host state.

Compliant state occurs under the following conditions:

- Target objects are compliant with the baselines and baseline groups when all updates in the baseline or baseline group are either installed on the target object, obsoleted by host, or are not applicable to the target object.
- The updates in a baseline are compliant when they are installed on the target object, or are not applicable to the object.

Non-Compliant

Non-compliant state indicates that one or more baselines in a baseline group, or one or more patches, extensions, or upgrades in a baseline are applicable to the target object, but are not installed (missing) on the target. You must remediate the target object to make it compliant.

When a baseline contains a non-compliant update, the overall status of the baseline is non-compliant. When a baseline group contains a non-compliant baseline, the overall status of the baseline group is non-compliant. The non-compliant state takes precedence over incompatible, unknown, and compliant states.

Unknown

When you attach a baseline or a baseline group to a vSphere object, and you do not scan the object, the state of the vSphere object against the baseline or baseline group is Unknown. This state indicates that a scan operation is required, that the scan has failed, or that you initiated a scan on an unsupported platform (for example, you performed a VMware Tools scan on a virtual machine running on an ESX 3.5 host).

When a baseline contains updates in compliant and unknown states, the overall status of the baseline is unknown. When a baseline group contains unknown baselines as well as compliant baselines, the overall status of the baseline group is unknown. The unknown compliance state takes precedence over compliant state.

Incompatible

Incompatible state requires attention and further action. You must determine the reason for incompatibility by probing further. You can remediate the objects in this state, but there is no guarantee that the operation will succeed. In most cases Update Manager provides sufficient details for incompatibility. For more information about incompatible compliance state, see Incompatible Compliance State.

When a baseline contains updates in incompatible, compliant, and unknown states, the overall status of the baseline is incompatible. When a baseline group contains incompatible, unknown, and compliant baselines, the overall status of the baseline group is incompatible. The incompatible compliance state takes precedence over compliant and unknown compliance states.

Viewing Patch Details

The **Patch Details** window displays a table of the patches ordered according to their compliance status with the selected virtual machine or host.

The compliance summary above the table in the **Patch Details** window represents the number of the applicable patches, missing patches (noncompliant), compliant patches, staged patches, and so on. If any of the patches are in the incompatible state, the compliance summary displays a detailed view of the incompatible patches. Incompatibility might be a result of a conflict, missing update packages, and so on.

You can obtain complete information about a patch by double-clicking a patch in the **Patch Details** window.

Table 8-2. Patch Details Window

Option	Description
Patch Name	Name of the update.
Vendor	Vendor of the update.
Compliance	Compliance status of the patch. The state might be Missing (Non-Compliant), Not Applicable, Unknown, Installed (Compliant), and so on.
Patch ID	Vendor-assigned identification code of the update.
Severity	Severity of the update. For hosts, the severity status might be Critical, General, Security, and so on. For virtual machines, the severity might be Critical, Important, Moderate, and so on.
Category	Category of the update. The category might be Security, Enhancement, Recall, Info, Other, and so on.
Impact	The action that you must take to apply the update. This action might include rebooting the system or putting the host into maintenance mode.
Release Date	Release date of the update.

Viewing Extension Details

The **Extension Details** window displays a table of the extensions in the order of their compliance status with the selected host.

You can obtain complete information about an extension by double-clicking an extension in the **Extension Details** window.

Table 8-3. Extension Details Window

Option	Description
Patch Name	Name of the update.
Vendor	Vendor of the update.
Compliance	Compliance status of the patch. The state might be Missing (Non-Compliant), Not Applicable, Unknown, Installed (Compliant), and so on.
Patch ID	Vendor-assigned identification code of the update.
Severity	Severity of the update. For hosts, the severity status might be Critical, General, Security, and so on. For virtual machines, the severity might be Critical, Important, Moderate, and so on.
Category	Category of the update. The category might be Security, Enhancement, Recall, Info, Other, and so on.
Impact	The action that you must take to apply the update. This action might include rebooting the system or putting the host into maintenance mode.
Release Date	Release date of the update.

Viewing Upgrade Details

The **Upgrade Details** window presents information about a specific upgrade you select.

Table 8-4. Host Upgrade Details Window

Option	Description
Baseline Name	Name of the upgrade baseline.
Baseline Type	The baseline type is host upgrade.
Baseline Description	Description of the baseline. If the baseline has no description, it is not displayed.
Compliance State	Compliance status for the upgrade. It represents a comparison between the state of the selected object and the upgrade baseline.
ESXi image	Displays the ESXi image included in the baseline.
Product	Displays the release version of the upgrade.
Version	Target version of the upgrade baseline.

Table 8-4. Host Upgrade Details Window (Continued)

Option	Description
Vendor	Vendor that provided the ESXi image.
Acceptance level	Acceptance level of the ESXi image and included software packages. ESXi images can be either Signed or Unsigned, indicating their level of acceptance by VMware. Software packages included in ESXi images have the following acceptance levels: **VMware Certified** The package has gone through a rigorous certification program that verifies the functionality of the feature, and is signed by VMware with a private key. VMware provides customer support for these packages. **VMware Accepted** The package has gone through a less rigorous acceptance test program that only verifies that the package does not destabilize the system, and is signed by VMware with a private key. The test regimen does not validate the proper functioning of the feature. VMware support will hand off support calls directly to the partner. **Partner Supported** The partner has signed an agreement with VMware and has demonstrated a sound test methodology. VMware provides a signed private/public key pair to the partner to use for self-signing their packages. VMware support will hand off support calls directly to the partner. **Community Supported** The package is either unsigned, or signed by a key that is not cross-signed by VMware. VMware does not provide support for the package. For support, customers must either utilize the community or contact the author of the package.

Table 8-5. VMware Tools and Virtual Machine Hardware Upgrade Details Window

Option	Description
Baseline Name	Name of the upgrade baseline.
Baseline Type	Type of the baseline. The values can be VMware Tools upgrade or virtual machine hardware upgrade.
Baseline Description	Description of the baseline.
Compliance State	Compliance status for the upgrade. It represents a comparison between the state of the selected object and the upgrade baseline.
VMware Tools Status	Status of VMware Tools on the machine.
Current Hardware Version	Hardware version of the virtual machine.
Target Hardware Version	Target hardware version of the virtual machine.

Host Upgrade Scan Messages in Update Manager

When you scan ESXi hosts against an upgrade baseline, Update Manager runs a precheck script and provides informative messages in the **Upgrade Details** window for each host. The messages notify you about potential problems with hardware, third-party software on the host, and configuration issues, which might prevent a successful upgrade to ESXi 6.7.

Messages that Update Manager provides correspond to error or warning codes from running the host upgrade precheck script.

For interactive installations and upgrades performed by using the ESXi installer, the errors or warnings from the precheck script are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations and upgrades, the errors or warnings are written to the installation log.

Update Manager provides scan result messages in the **Upgrade Details** window for errors or warnings from the precheck script. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan operation, review the Update Manager log file `C:\Documents and Settings\All Users\Application Data\VMware\VMware Update Manager\Logs\vmware-vum-server-log4cpp.log`.

Table 8-6. Scan Result Messages and Corresponding Error and Warning Codes

Scan Result Message in Update Manager	Description
`Host CPU is unsupported. New ESXi version requires a 64-bit CPU with support for LAHF/SAHF instructions in long mode.`	This message appears if the host processor is 32-bit and does not support required features. The corresponding error code is `64BIT_LONGMODESTATUS`.
`Trusted boot is enabled on the host but the upgrade does not contain the software package esx-tboot. Upgrading the host will remove the trusted boot feature.`	This message indicates that the host upgrade scan did not locate the `esx-tboot` VIB on the upgrade ISO. The corresponding error code is `TBOOT_REQUIRED`
`VMkernel and Service Console network interfaces are sharing the same subnet` *`subnet_name`*`. This configuration is not supported after upgrade. Only one interface should connect to subnet` *`subnet_name`*`.`	Warning. An IPv4 address was found on an enabled Service Console virtual NIC for which there is no corresponding address in the same subnet in the vmkernel. A separate warning appears for each such occurrence. The corresponding error code is `COS_NETWORKING`.
`New ESXi version requires a minimum of` *`core_count`* `processor cores.`	The host must have at least two cores. The corresponding error code is `CPU_CORES`.
`Processor does not support hardware virtualization or it is disabled in BIOS. Virtual machine performance may be slow.`	Host performance might be impaired if the host processor does not support hardware virtualization or if hardware virtualization is not turned on in the host BIOS. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation. The corresponding error code is `HARDWARE_VIRTUALIZATION`.
`Insufficient memory, minimum` *`size_in_MB`* `required for upgrade.`	The host requires the specified amount of memory to upgrade. The corresponding error code is `MEMORY_SIZE`.
`Host upgrade validity checks for` *`file_name`* `are not successful.`	This test checks whether the precheck script itself can be run. The corresponding error code is `PRECHECK_INITIALIZE`.
`The host partition layout is not suitable for upgrade.`	Upgrade is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition starts after sector 1843200. The corresponding error code is `PARTITION_LAYOUT`.

Table 8-6. Scan Result Messages and Corresponding Error and Warning Codes (Continued)

Scan Result Message in Update Manager	Description
`Unsupported configuration.`	The file `/etc/vmware/esx.conf` must exist on the host. This message indicates that the file /etc/vmware/esx.conf is either missing, or the file data cannot be retrieved or read correctly. The corresponding error code is `SANE_ESX_CONF`.
`The host does not have sufficient free space on a local VMFS datastore to back up current host configuration. A minimum of` *`size_in_MB`* `is required.`	The host disk must have enough free space to store the ESXi 5.x configuration between reboots. The corresponding error code is `SPACE_AVAIL_CONFIG`.
`The upgrade is not supported for current host version.`	Upgrading to ESXi 6.7 is possible only from ESXi 6.0 and ESXi 6.5 hosts. The corresponding error code is `SUPPORTED_ESX_VERSION`.
`Unsupported devices` *`device_name`* `found on the host.`	The script checks for unsupported devices. Some PCI devices are not supported with ESXi 6.7. The corresponding error code is `UNSUPPORTED_DEVICES`.
`Host software configuration requires a reboot. Reboot the host and try upgrade again.`	To ensure a good bootbank for the upgrade, you must reboot the hosts before remediation. The corresponding error code is `UPDATE_PENDING`.
In an environment with Cisco Nexus 1000V Distributed Virtual Switch, Update Manager displays different messages in different situations. For details, see Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present.	If Cisco's Virtual Ethernet Module (VEM) software is found on the host, the precheck script checks if the software is part of the upgrade as well, and that the VEM supports the same version of the Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the script returns a warning and the scan result indicates the version of the VEM software that was expected on the upgrade ISO, and the version, if any, that was found on the ISO. The corresponding error code is `DISTRIBUTED_VIRTUAL_SWITCH`.
`The host uses an EMC PowerPath multipathing module` *`file_name`* `to access storage. The host will not be able to access such storage after upgrade.`	The script checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the script verifies that matching components (CIM, VMkernel module) also exist in the upgrade. If they do not, the script returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found. The corresponding error code is `POWERPATH`.

Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present

When you scan a host that is managed by the Cisco Nexus 1000V virtual switch, host upgrade scan messages provide information about problems with compliance between the VEM modules installed on the host and the modules available on the ESXi 6.0 image.

Update Manager supports Cisco Nexus 1000V, a virtual access software switch that works with VMware vSphere and consists of two components.

Virtual Supervisor Module (VSM)
The control plane of the switch and a virtual machine that runs NX-OS.

Virtual Ethernet Module (VEM)
A virtual line card embedded in ESXi hosts.

Update Manager determines whether a host is managed by Cisco Nexus 1000V. Update Manager verifies whether Cisco Nexus 1000V VEM VIBs in the ESXi upgrade image are compatible with the Cisco Nexus 1000V VSM managing the host.

By using vSphere ESXi Image Builder, you can create custom ESXi images, which contain third-party VIBs that are required for a successful remediation operation.

Table 8-7. Host Upgrade Scan Messages for the Cisco Nexus 1000V network switch

Host Upgrade Scan Message	Description
`The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V software package on the host. Upgrading the host will remove the feature from the host.`	A VEM VIB is not available on the ESXi 6.0 upgrade image.
`The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade contains a Cisco Nexus 1000V software package` *VIB_name* `that is incompatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.`	The VEM VIB on the ESXi 6.0 upgrade image is not compatible with the version of the VSM.
`The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.`	The host and the image do not contain VEM VIBs, but the host is still listed in vCenter Server as managed by Cisco Nexus 1000V.
`Cannot determine whether the upgrade breaks Cisco Nexus 1000V virtual network switch feature on the host. If the host does not have the feature, you can ignore this warning.`	There was a problem with determining compatibility between the VEM VIB on the ESXi 6.0 upgrade image and the VSM. Check whether the version of the VSM managing the host is certified as being compatible with vCenter Server 6.0 and ESXi 6.0.

VMware Tools Status

For VMware Tools, the **Upgrade Details** window provides information about both compliance state and status. The status indicates whether the current version of VMware Tools is installed or supported and whether upgrades are available.

Table 8-8. VMware Tools Status

VMware Tools Status	Description	Compliance State
VMware Tools version is compliant.	The VMware Tools version is recent and supported. Remediation is not required.	Compliant
VMware Tools is installed, supported, and newer than the version available on the host.	VMware Tools is installed on a machine that is running on an earlier ESXi version. Remediation is not required.	Compliant
VMware Tools is installed and supported, but a newer version is available on the host.	An earlier supported version of VMware Tools is installed on the virtual machine. You can upgrade VMware Tools, but the existing earlier version is also supported.	Non-Compliant
VMware Tools is installed, but the installed version has a known issue and should be immediately upgraded.	A serious issue is present in the VMware Tools version that is installed on the machine. You must remediate the virtual machine against a VMware Tools upgrade baseline.	Non-Compliant
VMware Tools is installed, but the version is too new to work correctly with this virtual machine.	The existing newer version might cause problems on the virtual machine. You must remediate the virtual machine against a VMware Tools upgrade baseline, to downgrade to a supported version.	Non-Compliant
VMware Tools is installed, but the version is too old.	The VMware Tools version is no longer supported. You must remediate the virtual machine against a VMware Tools upgrade baseline.	Non-Compliant
VMware Tools is not installed.	VMware Tools is not present on the virtual machine. You must install VMware Tools by using the vSphere Web Client.	Incompatible
VMware Tools is not managed by vSphere.	VMware Tools is installed by using operating system specific packages that cannot be upgraded with Update Manager. To upgrade VMware Tools by using Update Manager, you must install VMware Tools from the vSphere Web Client.	Incompatible
Status is empty.	The virtual machine has not been scanned.	Unknown

Remediating vSphere Objects 9

You can remediate virtual machines and hosts using either user-initiated remediation or scheduled remediation at a time that is convenient for you.

If your vCenter Server is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can remediate only the inventory objects managed by the vCenter Server system with which Update Manager is registered.

To remediate vSphere objects, you need the **Remediate to Apply Patches, Extensions, and Upgrades** privilege. For more information about managing users, groups, roles, and permissions, see the *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see Update Manager Privileges.

This chapter includes the following topics:

Orchestrated Upgrades of Hosts and Virtual Machines

You can perform orchestrated upgrades of hosts or virtual machines in your vSphere inventory by using baseline groups. Baseline groups contain baselines for either hosts or virtual machines.

You can perform an orchestrated upgrade at the level of a container object or an individual object.

Orchestrated Upgrade of Hosts

Orchestrated upgrades let you apply upgrades, patches, and extensions to hosts in your inventory by using a single host baseline group.

If the baseline group contains an upgrade baseline, Update Manager first upgrades the hosts and then applies the patch or extension baselines. Because the upgrade runs first and patches are applicable to a specific host version, the orchestrated workflow ensures that patches are not lost during the upgrade.

Orchestrated Upgrade of Virtual Machines

You can use an orchestrated upgrade to upgrade the virtual machine hardware and VMware Tools of all the virtual machines in the vSphere inventory at the same time, using baseline groups containing the following baselines:

- VM Hardware Upgrade to Match Host
- VMware Tools Upgrade to Match Host

Upgrading the virtual hardware of the virtual machines exposes new devices and capabilities to the guest operating systems. You must upgrade VMware Tools before upgrading the virtual hardware version so that all required drivers are updated in the guest. You cannot upgrade the virtual hardware of the virtual machines if VMware Tools is not installed, is out of date, or is managed by third-party tools.

When you upgrade virtual machines against a baseline group containing the VM Hardware Upgrade to Match Host baseline and the VMware Tools Upgrade to Match Host baseline, Update Manager sequences the upgrade operations in the correct order, and VMware Tools is upgraded first.

During the upgrade of VMware Tools, the virtual machines must be powered on. If a virtual machine is in the powered off or suspended state before remediation, Update Manager powers it on. After the upgrade completes, Update Manager restarts the machine and restores the original power state of the virtual machine.

During the virtual hardware upgrade, the virtual machines must be shut down. If a virtual machine is powered on, Update Manager powers the machine off, upgrades the virtual hardware, and then powers the virtual machine on.

Remediating Hosts

Host remediation runs in different ways depending on the types of baselines you attach and whether the host is in a cluster or not.

Remediation of Hosts in a Cluster

For ESXi hosts in a cluster, the remediation process is sequential by default. With Update Manager, you can select to run host remediation in parallel.

When you remediate a cluster of hosts sequentially and one of the hosts fails to enter maintenance mode, Update Manager reports an error, and the process stops and fails. The hosts in the cluster that are remediated stay at the updated level. The ones that are not remediated after the failed host remediation are not updated. If a host in a DRS enabled cluster runs a virtual machine on which Update Manager or vCenter Server are installed, DRS first attempts to migrate the virtual machine running vCenter Server or Update Manager to another host, so that the remediation succeeds. In case the virtual machine cannot be migrated to another host, the remediation fails for the host, but the process does not stop. Update Manager proceeds to remediate the next host in the cluster.

The host upgrade remediation of ESXi hosts in a cluster proceeds only if all hosts in the cluster can be upgraded.

Remediation of hosts in a cluster requires that you temporarily disable cluster features such as VMware DPM and HA admission control. Also, turn off FT if it is enabled on any of the virtual machines on a host, and disconnect the removable devices connected to the virtual machines on a host, so that they can be migrated with vMotion. Before you start a remediation process, you can generate a report that shows which cluster, host, or virtual machine has the cluster features enabled. For more information, see Pre-Check Remediation Report.

Note When you perform remediation on a cluster that consists of not more than two hosts, disabling HA admission control might not be enough to ensure successful remediation. You might need to disable vSphere Availability (HA) on the cluster. If you keep HA enabled, remediation attempts on host in the cluster fail, because HA cannot provide recommendation to Update Manager to place any of the hosts into maintenance mode. The reason is that if one of the two hosts is placed into maintenance mode there is no failover host left available in the cluster. To ensure successful remediation on a 2-node cluster, disable HA on the cluster or place the hosts in maintenance mode manually and then perform remediate the two host in the cluster.

When you remediate a cluster of hosts in parallel, Update Manager remediates multiple hosts concurrently. During parallel remediation, if Update Manager encounters an error when remediating a host, it ignores the host and the remediation process continues for the other hosts in the cluster. Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number.

Update Manager remediates hosts that are part of a vSAN cluster sequentially even if you select the option to remediate them in parallel. The reason is that by design only one host from a vSAN cluster can be in a maintenance mode at any time.

For multiple clusters under a data center, the remediation processes run in parallel. If the remediation process fails for one of the clusters within a data center, the remaining clusters are still remediated.

Remediation Against Baseline Groups

When you remediate hosts against baseline groups containing an upgrade baseline and patch or extension baselines, the upgrade is performed first.

Host Upgrade Remediation

When you upgrade an ESXi 6.0 and ESXi 6.5 host to ESXi 6.7, all supported custom VIBs remain intact on the host after the upgrade, regardless of whether the VIBs are included in the installer ISO. This is because ESXi 6.x hosts are binary compatible.

You can upgrade hosts by using custom ESXi images that contain third-party modules for ESXi 6.7. In such a case, third-party modules that are compatible with ESXi 6.7 stay available on the upgraded host.

Host upgrade in a high-latency network in which Update Manager and the hosts are at different locations might take a few hours because the upgrade file is copied from the Update Manager server repository to the host before the upgrade. During this time, the host stays in maintenance mode.

Update Manager 6.7 supports upgrade from ESXi 6.0.x and ESXi 6.5.x to ESXi 6.7.

Important After you have upgraded your host to ESXi 6.7, you cannot roll back to your version ESXi 6.0.x or ESXi 6.5.x software. Back up your host configuration before performing an upgrade. If the upgrade fails, you can reinstall the ESXi 6.0.x or ESXi 6.5.x software that you upgraded from, and restore your host configuration. For more information about backing up and restoring your ESXi configuration, see *vSphere Upgrade*.

Host Patch Remediation

Update Manager handles host patches in the following ways:

- If a patch in a patch baseline requires the installation of another patch, Update Manager detects the prerequisite in the patch repository and installs it together with the selected patch.
- If a patch is in a conflict with other patches that are installed on the host, the conflicting patch might not be staged or installed. However, if another patch in the baseline resolves the conflicts, the conflicting patch is installed. For example, consider a baseline that contains patch A and patch C, and patch A conflicts with patch B, which is already installed on the host. If patch C obsoletes patch B, and patch C is not in a conflict with patch A, the remediation process installs patches A and C.
- If a patch is in a conflict with the patches in the Update Manager patch repository and is not in a conflict with the host, after a scan, Update Manager reports this patch as a conflicting one. You can stage and apply the patch to the host.
- When multiple versions of the same patch are selected, Update Manager installs the latest version and skips the earlier versions.

During patch remediation, Update Manager automatically installs the prerequisites of patches.

With Update Manager 6.7, you can remediate hosts of version ESXi 6.0 and ESXi 6.5 against offline bundles that you have imported manually.

You can stage patches before remediation to reduce host downtime.

Host Extension Remediation

During extension remediation, Update Manager does not automatically install the prerequisites of the extension. This might cause some remediation operations to fail. If the missing prerequisite is a patch, you can add it to a patch baseline. If the missing prerequisite is an extension, you can add it to the same or another extension baseline. You can then remediate the host against the baseline or baselines that contain the prerequisite and the original extension.

Remediation of PXE Booted ESXi Hosts

Update Manager lets you remediate PXE booted ESXi hosts. Update Manager does not apply patches that require a reboot to PXE booted ESXi hosts.

If there is any additional software installed on the PXE booted ESXi host, the software might be lost if the host restarts. Update your image profile with the additional software so that it will be present after the reboot.

Staging Patches and Extensions to ESXi Hosts

Staging allows you to download the patches and extensions from the Update Manager server to the ESXi hosts, without applying the patches and extensions immediately. Staging patches and extensions speeds up the remediation process because the patches and extensions are already available locally on the hosts.

To stage patches or extensions to hosts, first attach a patch or extension baseline or a baseline group containing patches and extensions to the host.

You can reduce the downtime during remediation, by staging patches and extensions whose installation requires that a host enters maintenance mode. Staging patches and extensions itself does not require that the hosts enter maintenance mode.

Patches cannot be staged if they are obsoleted by patches in the baselines or baseline groups for the same stage operation. Update Manager stages only patches that it can install in a subsequent remediation process, based on the present scan results of the host. If a patch is obsoleted by patches in the same selected patch set, the obsoleted patch is not staged.

If a patch is in conflict with the patches in the Update Manager patch repository and is not in conflict with the host, after a scan, Update Manager reports this patch as a conflicting one. You can stage the patch to the host and after the stage operation, Update Manager reports this patch as staged.

During the stage operation, Update Manager performs prescan and postscan operations, and updates the compliance state of the baseline.

After you stage patches or extensions to hosts, you should remediate the hosts against all staged patches or extensions.

After a successful remediation of hosts, the host deletes all staged patches or extensions from its cache regardless of whether they were applied during the remediation. The compliance state of patches or extensions that were staged but not applied to the to the hosts reverts from Staged to its previous value.

Important Staging patches and extensions is supported for hosts that are running ESXi 6.0 and later. You can stage patches to PXE booted ESXi hosts, but if the host is restarted prior to remediation, the staged patches will be lost and you will have to stage them again.

Stage Patches and Extensions to ESXi Hosts

Download the patches and extensions from the Update Manager server to the ESXi hosts. Staging lets you reduce the time the host spends in maintenance mode during remediation.

Prerequisites

- Attach a patch or extension baseline or a baseline group containing patches and extensions to the host.

- Required privileges: **VMware vSphere Update Manager.Manage Patches and Upgrades.Stage Patches and Extensions**.

For a list of Update Manager privileges and their descriptions, see Update Manager Privileges.

Procedure

1. Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2. Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3. Select **Menu > Hosts and Clusters**, and select a host or a cluster from the vSphere inventory.
4. Select the **Updates** tab.

   You are in the Update Manager compliance view.

5. Select a patch or extension baseline.
6. Click **Stage**.

   The **Stage Patches** wizard opens.

7. Select the hosts where patches and extensions to download.

   The number of selected hosts appears on top of the list.

8. Under **Install** section, you can view the patches or extensions that will download to the selected hosts.
9. Click **OK**.

The staging operation starts. You can monitor the progress of the task under the **Recent Tasks** pane.

What to do next

Remediate the host or hosts.

After a remediation is successfully completed, all staged patches and extensions, whether installed or not during the remediation, are deleted from the host.

Stage Patches and Extensions to ESXi Hosts in the vSphere Web Client

Download the patches and extensions from the Update Manager server to the ESXi hosts. Staging lets you reduce the time the host spends in maintenance mode during remediation.

Prerequisites

- Attach a patch or extension baseline or a baseline group containing patches and extensions to the host.

- Required privileges: **VMware vSphere Update Manager.Manage Patches and Upgrades.Stage Patches and Extensions**.

Procedure

1. Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.
2. From the inventory object navigator, select a data center, a cluster, or a host, and click the **Update Manager** tab.
3. Click **Stage**.

   The **Stage Patches** wizard opens.
4. On the **Baseline Selection** page of the **Stage** wizard, select the patch and extension baselines to stage.
5. Select the hosts where patches and extensions to download, and click **Next**.

   If you select to stage patches and extensions to a single host, it is selected by default.
6. (Optional) Deselect the patches and extensions to exclude from the stage operation.
7. (Optional) To search within the list of patches and extensions, type a search criteria in the text box in the upper-right corner.
8. Click **Next**.
9. Review the **Ready to Complete** page, and click **Finish**.

The number of the staged patches and extensions for the specific host is displayed in the Patches and Extensions columns in the bottom pane of the **Update Manager** tab.

What to do next

Remediate the host or hosts.

After a remediation is successfully completed, all staged patches and extensions, whether installed or not during the remediation, are deleted from the host.

Remediation Specifics of ESXi Hosts

For ESXi hosts, updates are all-inclusive. The most recent update contains the patches from all previous releases.

The ESXi image on the host maintains two copies. The first copy is in the active boot and the second one is in the standby boot. When you patch an ESXi host, Update Manager creates an image based on the content of the active boot and the content of the patch. The new ESXi image is then located in the standby boot and Update Manager designates the active boot as the standby boot and reboots the host. When the ESXi host reboots, the active boot contains the patched image and the standby boot contains the previous version of the ESXi host image.

When you upgrade an ESXi host, Update Manager replaces the backup image of the host with the new image and replaces the active boot and the standby boot. During the upgrade, the layout of the disk hosting the boots changes. The total disk space for an ESXi host remains 1GB, but the disk partition layout within that 1GB disk space changes to accommodate the new size of the boots where the ESXi 6.0 images to be stored.

For purposes of rollback, the term update refers to all ESXi patches, updates, and upgrades. Each time you update an ESXi host, a copy of the previous ESXi build is saved on your host.

If an update fails and the ESXi 6.7 host cannot boot from the new build, the host reverts to booting from the original boot build. ESXi permits only one level of rollback. Only one previous build can be saved at a time. In effect, each ESXi 6.7 host stores up to two builds, one boot build and one standby build.

Remediation of ESXi 6.0 and 6.5 hosts to their respective ESXi update releases is a patching process, while the remediation of ESXi hosts from version 6.0 or 6.5 to 6.7 is an upgrade process.

Update Manager 6.7 supports upgrade from ESXi 6.0.x and ESXi 6.5.x to ESXi 6.7.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-6.7.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder.

Any third-party software modules on a ESXi 6.7 host will remain intact after upgrade to ESXi 6.5.

Note In case of an unsuccessful upgrade from ESXi 6.0 or ESXi 6.5 to ESXi 6.7, you cannot roll back to your previous ESXi 6.0 or ESXi 6.5 instance.

From the Update Manager settings, you can configure the host remediation process to skip a host reboot during host patch and host upgrade operations. The configuration setting is Quick Boot and is available in the hosts and clusters settings of Update Manager.

Functionality Differences Between Remediation Process in the vSphere Client and the vSphere Web Client

---

Note The functionality of the remediation wizard differs between the vSphere Client and the vSphere Web Client. To change any of the host and cluster remediation settings, you must change the default Update Manager settings from the vSphere Web Client, or use the remediation wizard in the vSphere Web Client and save the host and cluster settings that you apply as default.

Remediating Hosts That Contain Third-Party Software

Hosts might contain third-party software, such as Cisco Nexus 1000V VEMs or EMC PowerPath modules. When you upgrade an ESXi 6.0 or ESXi 6.5 host to ESXi 6.5, all supported custom VIBs are migrated, regardless of whether the VIBs are included in the installer ISO.

If the host or the installer ISO image contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the VIB that created the conflict.

To discover potential problems with third-party software before an upgrade operation, scan the hosts against an upgrade baseline and review the scan messages in the Update Manager Compliance view. See Host Upgrade Scan Messages in Update Manager and Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present.

For information about upgrading with third-party customization, see the *vSphere Upgrade* documentation. For information about using vSphere ESXi Image Builder to make a custom ISO, see the *vSphere Installation and Setup* documentation.

Remediating ESXi 6.0 or ESXi 6.5 Hosts Against ESXi 6.7 Image

When you upgrade an ESXi 6.0 or ESXi 6.5 host to ESXi 6.7, all supported custom VIBs remain intact on the host after the upgrade, regardless of whether the VIBs are included in the installer ISO.

When you perform a host scan, the target host is scanned against a set of VIBs from the upgrade image. If you scan hosts against an upgrade baseline that contains an ISO image of the same version as the target host, Update Manager displays Compliant or Non-compliant scan result. If the upgrade image is the basic one distributed by VMware, or is a custom ISO image that contains the same set of VIBs as the ones already installed on the target host, the scan result is Compliant. If the upgrade ISO contains VIBs that are of different kind or version than the target host, the scan result is Non-compliant.

The remediation process of ESXi 6.0 or ESXi 6.5 host to ESXi 6.5 image is an upgrade process.

You can also use an ISO 6.7 image in an upgrade operation of an ESXi 6.5 host. The remediation process of ESXi 6.7 host by using ESXi 6.7 image with additional VIBs is equivalent to a patching process. Because the upgrade image is of the same version as the target host, with completing the upgrade operation the additional VIBs are added to the target host.

Table 9-1. Scan and Remediation Situations for ESXi 6.0 and ESXi 6.5 Hosts Against ESXi 6.7 Images

Action	Description
Scan and remediation of ESXi 6.0 or ESXi 6.5 hosts against ESXi 6.7 image that contains additional non-conflicting and non-obsoleting VIBs with the target host.	Update Manager displays Non-Compliant scan result. Remediation succeeds. All VIBs on the target host before remediation remain on the host. All VIBs from the upgrade image that are not present on the target host before remediation are added to the host.
Scan and remediation of ESXi 6.0 or ESXi 6.5 hosts against ESXi 6.7 image that contains VIBs of later version than the same VIBs on the target host.	Update Manager displays Non-Compliant scan result. Remediation succeeds. VIBs on the target host are updated to the later version.
Scan and remediation of ESXi 6.0 or ESXi 6.5 hosts against ESXi 6.7 image that contains conflicting VIBs with the target host.	Update Manager displays Incompatible scan result. Remediation fails. The host remains intact.

Table 9-1. Scan and Remediation Situations for ESXi 6.0 and ESXi 6.5 Hosts Against ESXi 6.7 Images (Continued)

Action	Description
Scan and remediation of ESXi 6.0 or ESXi 6.5 hosts against ESXi 6.7 image that contains vendor-tagged VIBs.	■ If the vendor-tagged VIBs do not match the host hardware, Update Manager displays Incompatible scan result. Remediation fails. ■ If the vendor-tagged VIBs match the host hardware, Update Manager displays Non-Compliant scan result and remediation succeeds.
Scan and remediation of ESXi 6.0 or ESXi 6.5 hosts against an ESXi 6.7 image that contains VIBs that obsolete the VIBs installed on the host.	Remediation succeeds. All VIBs that have been installed on the target host before remediation are replaced by the newer VIBs from the ESXi image.

Remediation Specifics of Hosts That Are Part of a vSAN Cluster

There are some specifics about remediating hosts that are part of a vSAN cluster.

Maintenance Mode Specifics of vSAN Clusters

By design only one host from a vSAN cluster can be in a maintenance mode at any time. Because of that the host remediation process might take extensive amount of time to complete since Update Manager must handle the remediation of the hosts sequentially. Update Manager remediates hosts that are part of a vSAN cluster sequentially even if you select the option to remediate them in parallel.

If the vSAN cluster has a system-managed baseline attached by default, you can remediate the cluster against the baseline to bring all the hosts in a compliant state, and install the latest software recommended by vSAN.

You have several ways to remediate a host that is part of a vSAN cluster, depending on how you want the virtual machines handled on the host:

- You can put the host in maintenance mode manually, and remediate the host by using Update Manager.
- You can have a host entering maintenance mode during the Update Manager remediation process.

From the vSphere Web Client you can select between multiple options when putting a host from a vSAN cluster in maintenance mode: Ensure accessibility, Full data evacuation, and No data evacuation. The Ensure accessibility option is the default option, and means that when you put a host in maintenance mode, the vSAN ensures that all accessible virtual machines on this host remain accessible. To learn more about each of the options, see the *Place a Member of vSAN Cluster in Maintenance Mode* topic from *vSphere Storage* guide.

When you put a host from a vSAN cluster into maintenance mode, you must confirm a maintenance mode warning message. Before confirming the message, you can select to move powered off and suspended virtual machines to other hosts in the cluster, but you have no options on how to handle the powered on virtual machines on the host. The powered on virtual machines are automatically handled equivalently to the default Ensure accessibility option.

When you use Update Manager, the remediation process might put the host from the vSAN cluster in maintenance mode, which handles the virtual machines on the host in the manner of the default Ensure accessibility option.

If a host is a member of a vSAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because vSAN has to migrate the virtual machine data from one disk to another in the vSAN datastore cluster. Delays might take up to hours. You can work around this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the vSAN datastore.

Remediating vSAN Clusters Against System Managed Baselines

vSAN creates system managed baselines that you can use with Update Manager to upgrade the hosts in vSAN clusters to the latest supported ESXi version, patch the hosts with critical patches, and install drivers.

The system managed baselines appear automatically in Update Manager Compliance view if you are using vSAN clusters that contain hosts of ESXi version 6.0 Update 2 and later. If your vSphere environment does not contain any vSAN clusters, no system managed baselines are generated.

System baselines can be any of the following types:

- Upgrade baseline that consists of the latest supported ESXi upgrade image for your vSAN cluster.
- Patch baseline that consists of recommended critical patches for the ESXi hosts in your vSAN cluster.
- Driver baseline that consists of recommended drivers for the ESXi hosts in your vSAN cluster.

You cannot edit or delete a system managed baseline. You also cannot add it to custom baseline groups.

A combination between a patch, a driver, or an upgrade system managed baseline is automatically bundled in a vSAN system baseline group. For each vSAN cluster in the vSphere inventory, Update Manager displays a single system baseline group.

Update Manager runs automatic check once every 24 hours and downloads any new critical patches, drivers, or upgrade images related to vSAN that are available on VMware Cloud. VMware Cloud stores the Hardware Compatibility List for vSAN and the vSAN release catalog. After refreshing the baselines, Update Manager automatically performs a scan operation on the vSAN clusters against the updated system baselines.

Operations such as adding and removing hosts from an existing vSAN cluster also trigger refresh of the attached system baseline, followed by a scan operation of the cluster.

If the vSAN cluster is in compliant state, no further actions are needed.

If the vSAN cluster is in non-compliant state against the system baseline, Update Manager does not automatically initiate remediation. You decide when to remediate the cluster, and can start the process manually.

System Requirements for Using vSAN System Managed Baselines

- vCenter Server 6.5 Update 1 that runs on Windows.
- Update Manager 6.5 Update 1 that runs Windows and is connected to vCenter Server 6.5 Update 1.
- vSAN cluster that contains hosts of ESXi version 6.0 Update 2 and later.
- Constant access of the Update Manager host machine to the Internet.
- Account in the My VMware portal (my.vmware.com) to access VMware Cloud.

Remediate Hosts Against Patch or Extension Baselines

You can remediate hosts against attached patch or extension baselines.

With the vSphere Client, you can start remediation of a host or a cluster against a single baseline. To remediate a host or a cluster against multiple baselines, despite if the baselines are of the same type or of different types, you must create a baseline group.

Note The functionality of the remediation wizard differs between the vSphere Client and the vSphere Web Client. To change any of the host and cluster remediation settings, you must change the default Update Manager settings from the vSphere Web Client, or use the remediation wizard in the vSphere Web Client and save the host and cluster settings that you apply as default.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Patches and Upgrades.Remediate to Apply Patches, Extensions, and Upgrades**.

Procedure

1. Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2. Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3. Select **Menu > Hosts and Clusters**, and select a host or a cluster from the vSphere inventory.
4. Select the **Updates** tab.

   You are in the Update Manager compliance view.

5. Select a patch or extension baseline.
6. Click **Remediate**.

   The **Remediate** wizard opens.

7. Select the hosts to remediate.

8 Under Install, view the patches and extensions included in the baseline or the baseline group.

9 Under Remediation settings, view the predefined host and cluster settings for the remediation operation.

10 Click **OK** to start remediation on the hosts.

Remediate Hosts Against Patch or Extension Baselines in the vSphere Web Client

You can remediate hosts against attached patch or extension baselines.

The remediation process for host extension baselines is similar to the remediation process for host patch baselines. You can remediate a host against a single baseline or multiple baselines of the same type. To remediate against baselines of different types, you must create a baseline group. For more information about remediating hosts against baseline groups containing host upgrade, patch, and extension baselines, see Remediate Hosts Against Baseline Groups in the vSphere Web Client.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 Select **Home > Hosts and Clusters**.

3 From the inventory object navigator, select a data center, a cluster, or a host, and click the **Update Manager** tab.

4 Click **Remediate**.

   If you selected a container object, all hosts under the selected object are remediated.

   The Remediate wizard opens.

5 From the Individual Baselines by Type, select **Patch Baselines** or **Extension Baselines** depending on what type of update you want to perform on the host.

6 Select the target hosts that you want to remediate and click **Next**.

   If you have chosen to remediate a single host and not a container object, the host is selected by default.

7 (Optional) On the Patches and Extensions page, deselect specific patches or extensions to exclude them from the remediation process, and click **Next**.

8 (Optional) On the Advanced options page, select the option to schedule the remediation to run later, and specify a unique name and an optional description for the task.

   The time you set for the scheduled task is the time of the vCenter Server instance to which Update Manager is connected.

9 (Optional) On the Advanced options page, select the option to ignore warnings about unsupported devices on the host, or no longer supported VMFS datastore to continue with the remediation.

10 Click **Next**.

11 (Optional) Enable Quick Boot to skip hardware reboot of the host after remediation, or deselect the check box if you want your host to undergo hardware reboot.

Quick Boot is a configuration setting that might be enabled by default from the Update Manager host and cluster settings.

Note Quick Boot is supported on a limited number of hardware configurations. For more information, see https://kb.vmware.com/s/article/52476.

12 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines before remediation.
Suspend virtual machines	Suspend all running virtual machines before remediation.
Do Not Change VM Power State	Leave virtual machines in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

13 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

14 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

15 (Optional) Select the check box under PXE Booted Hosts to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

16 (Optional) Save the host remediation options you selected as default.

Saves your current selections and makes them available as pre-selected for your next host remediation operation.

17 Click **Next**.

18 If you remediate hosts in a cluster, edit the cluster remediation options, and click **Next**.

The Cluster remediation options page is available only when you remediate clusters.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled. This affects all fault tolerant virtual machines in the selected clusters.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. You can select one of the following options for parallel remediation: ■ You can let Update Manager continuously evaluate the maximum number of hosts it can remediate concurrently without disrupting DRS settings. ■ You can specify a limit of the number of concurrently remediated hosts in each cluster you remediate. **Note** Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **VM Power State** menu in the Maintenance Mode Options pane on the Host Remediation Options page. By design only one host from a vSAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a vSAN cluster sequentially even if you select the option to remediate them in parallel.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

19 (Optional) Save the cluster remediation options you selected as default.

Saves your current selections and makes them available as pre-selected for your next cluster remediation operation.

20 (Optional) On the Ready to complete page, click **Pre-check Remediation** to generate a cluster remediation options report, and click **OK**.

   A Cluster Remediation Options Report dialog box opens. You can export this report, or copy the entries for your own record.

21 Review the Ready to Complete page, and click **Finish**.

Remediate Hosts Against an Upgrade Baseline

You can remediate ESXi hosts against a single attached upgrade baseline at a time. You can upgrade all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 6.7 image.

Note The functionality of the remediation wizard differs between the vSphere Client and the vSphere Web Client. To change any of the host and cluster remediation settings, you must change the default Update Manager settings from the vSphere Web Client, or use the remediation wizard in the vSphere Web Client and save the host and cluster settings that you apply as default.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Patches and Upgrades.Remediate to Apply Patches, Extensions, and Upgrades**.
- Attach a baseline that contains an ESXi 6.7 upgrade image to the host or the cluster.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

   Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

   The Update Manager administrative home view opens.

3 Select **Menu > Hosts and Clusters**, and select a host or a cluster from the vSphere inventory.

4 Select the **Updates** tab.

   You are in the Update Manager compliance view.

5 Select an upgrade baseline.

6 Click **Remediate**.

   The **Remediate** wizard opens.

7 Accept the terms in the license agreement, and click **OK**.

8 Select the hosts to remediate.

9 Under Install, view the patches and extensions included in the baseline or the baseline group.

10 Under Remediation settings, view the predefined host and cluster settings for the remediation operation.

11 Click **OK** to start remediation on the hosts.

Remediate Hosts Against an Upgrade Baseline in the vSphere Web Client

You can remediate ESXi hosts against a single attached upgrade baseline at a time. You can upgrade all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 6.7 image .

Note Alternatively, you can upgrade hosts by using a baseline group. See Remediate Hosts Against Baseline Groups in the vSphere Web Client.

Update Manager 6.7 supports upgrade from ESXi 6.0.x and ESXi 6.5.x to ESXi 6.7.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-6.7.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder.

Any third-party software modules on a ESXi 6.7 host will remain intact after upgrade to ESXi 6.5.

Note In case of an unsuccessful upgrade from ESXi 6.0 or ESXi 6.5 to ESXi 6.7, you cannot roll back to your previous ESXi 6.0 or ESXi 6.5 instance.

Prerequisites

To remediate a host against an upgrade baseline, attach the baseline to the host.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 Select **Home > Hosts and Clusters**.

3 From the inventory object navigator, select a data center, a cluster, or a host, and click the **Update Manager** tab.

4 Click **Remediate**.

   If you selected a container object, all hosts under the selected object are remediated.

   The Remediate wizard opens.

5 On the Select baselines page of the Remediate wizard, from the Individual Baselines by Type section, select **Upgrade Baselines**, and select the upgrade baseline to apply.

6 Select the target hosts that you want to remediate and click **Next**.

   If you have chosen to remediate a single host and not a container object, the host is selected by default.

7 On the End User License Agreement page, accept the terms, and click **Next**.

8 (Optional) On the Advanced options page, select the option to schedule the remediation to run later, and specify a unique name and an optional description for the task.

The time you set for the scheduled task is the time of the vCenter Server instance to which Update Manager is connected.

9 (Optional) On the Advanced options page, select the option to ignore warnings about unsupported devices on the host, or no longer supported VMFS datastore to continue with the remediation.

10 Click **Next**.

11 (Optional) Enable Quick Boot to skip hardware reboot of the host after remediation, or deselect the check box if you want your host to undergo hardware reboot.

Quick Boot is a configuration setting that might be enabled by default from the Update Manager host and cluster settings.

Note Quick Boot is supported on a limited number of hardware configurations. For more information, see https://kb.vmware.com/s/article/52476.

12 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines before remediation.
Suspend virtual machines	Suspend all running virtual machines before remediation.
Do Not Change VM Power State	Leave virtual machines in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

13 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

14 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

15 (Optional) Select the check box under PXE Booted Hosts to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

16 (Optional) Save the host remediation options you selected as default.

Saves your current selections and makes them available as pre-selected for your next host remediation operation.

17 Click **Next**.

18 If you remediate hosts in a cluster, edit the cluster remediation options, and click **Next**.

The Cluster remediation options page is available only when you remediate clusters.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled. This affects all fault tolerant virtual machines in the selected clusters.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.

Option	Details
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. You can select one of the following options for parallel remediation: ■ You can let Update Manager continuously evaluate the maximum number of hosts it can remediate concurrently without disrupting DRS settings. ■ You can specify a limit of the number of concurrently remediated hosts in each cluster you remediate. **Note** Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **VM Power State** menu in the Maintenance Mode Options pane on the Host Remediation Options page. By design only one host from a vSAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a vSAN cluster sequentially even if you select the option to remediate them in parallel.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

19 (Optional) Save the cluster remediation options you selected as default.

Saves your current selections and makes them available as pre-selected for your next cluster remediation operation.

20 (Optional) On the Ready to complete page, click **Pre-check Remediation** to generate a cluster remediation options report, and click **OK**.

A Cluster Remediation Options Report dialog box opens. You can export this report, or copy the entries for your own record.

21 Review the Ready to Complete page, and click **Finish**.

Note In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

Remediate Hosts Against Baseline Groups

You can perform an orchestrated upgrade by using a host baseline group. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

Prerequisites

- Required privileges: **VMware vSphere Update Manager.Manage Patches and Upgrades.Remediate to Apply Patches, Extensions, and Upgrades**.

Procedure

1 Use the vSphere Client to log in to a vCenter Server Appliance.

Note In vSphere 6.7, you cannot use the vSphere Client to connect to a vCenter Server instance that runs on Windows.

2 Click **Menu > Update Manager**.

The Update Manager administrative home view opens.

3 Select **Menu > Hosts and Clusters**, and select a host or a cluster from the vSphere inventory.

4 Select the **Updates** tab.

You are in the Update Manager compliance view.

5 Select a baseline group.

The upgrade baseline in the baseline group runs first, followed by patch and extension baselines.

6 Click **Remediate**.

The **Remediate** wizard opens.

7 If the baseline group includes an upgrade baseline, accept the terms in the license agreement, and click **OK**.

8 Select the hosts to remediate.

9 Under Install, view the patches and extensions included in the baseline or the baseline group.

10 Under Remediation settings, view the predefined host and cluster settings for the remediation operation.

11 Click **OK** to start remediation on the hosts.

Remediate Hosts Against Baseline Groups in the vSphere Web Client

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

You can perform an orchestrated upgrade by using a host baseline group. The upgrade baseline in the baseline group runs first, followed by patch and extension baselines.

Note Alternatively, you can upgrade hosts by using a single upgrade baseline. See Remediate Hosts Against an Upgrade Baseline in the vSphere Web Client.

Prerequisites

Ensure that at least one baseline group is attached to the host.

Review any scan messages in the **Upgrade Details** window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade to ESXi 6.7.

Procedure

1 Use the vSphere Web Client to log in to a vCenter Server Appliance, or to a vCenter Server system with which Update Manager is registered.

2 Select **Home > Hosts and Clusters**.

3 From the inventory object navigator, select a data center, a cluster, or a host, and click the **Update Manager** tab.

4 Click **Remediate**.

   If you selected a container object, all hosts under the selected object are remediated.

   The Remediate wizard opens.

5 On the Select baseline page of the **Remediate** wizard, select the baseline group and baselines to apply.

6 Select the target hosts that you want to remediate and click **Next**.

   If you have chosen to remediate a single host and not a container object, the host is selected by default.

7 On the End User License Agreement page, accept the terms, and click **Next**.

8 (Optional) On the Patches and Extensions page, deselect specific patches or extensions to exclude them from the remediation process, and click **Next**.

9 (Optional) On the Advanced options page, select the option to schedule the remediation to run later, and specify a unique name and an optional description for the task.

   The time you set for the scheduled task is the time of the vCenter Server instance to which Update Manager is connected.

10 (Optional) On the Advanced options page, select the option to ignore warnings about unsupported devices on the host, or no longer supported VMFS datastore to continue with the remediation.

11 Click **Next**.

12 (Optional) Enable Quick Boot to skip hardware reboot of the host after remediation, or deselect the check box if you want your host to undergo hardware reboot.

   Quick Boot is a configuration setting that might be enabled by default from the Update Manager host and cluster settings.

   Note Quick Boot is supported on a limited number of hardware configurations. For more information, see https://kb.vmware.com/s/article/52476.

13 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines before remediation.
Suspend virtual machines	Suspend all running virtual machines before remediation.
Do Not Change VM Power State	Leave virtual machines in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

14 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

15 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

16 (Optional) Select the check box under PXE Booted Hosts to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

17 (Optional) Save the host remediation options you selected as default.

Saves your current selections and makes them available as pre-selected for your next host remediation operation.

18 Click **Next**.

19 If you remediate hosts in a cluster, edit the cluster remediation options, and click **Next**.

The Cluster remediation options page is available only when you remediate clusters.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled. This affects all fault tolerant virtual machines in the selected clusters.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. You can select one of the following options for parallel remediation: ■ You can let Update Manager continuously evaluate the maximum number of hosts it can remediate concurrently without disrupting DRS settings. ■ You can specify a limit of the number of concurrently remediated hosts in each cluster you remediate. **Note** Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the **VM Power State** menu in the Maintenance Mode Options pane on the Host Remediation Options page. By design only one host from a vSAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a vSAN cluster sequentially even if you select the option to remediate them in parallel.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

20 (Optional) Save the cluster remediation options you selected as default.

Saves your current selections and makes them available as pre-selected for your next cluster remediation operation.

21 (Optional) On the Ready to complete page, click **Pre-check Remediation** to generate a cluster remediation options report, and click **OK**.

A Cluster Remediation Options Report dialog box opens. You can export this report, or copy the entries for your own record.

22 Review the Ready to Complete page, and click **Finish**.

Note In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

Pre-Check Remediation Report

The **Pre-Check Remediation** is a check that is performed on the host or the cluster that displays a table that lists possible problems that might prevent a successful remediation, and a recommendation on how to fix the issues.

When you generate a pre-check remediation report, Update Manager generates a list with recommended actions you must perform to ensure a successful remediation of the hosts in your cluster.

You can generate a pre-check remediation report from both vSphere Client and the vSphere Web Client.

From the vSphere Client, you can generate a pre-check remediation report by selecting a host or a cluster from the inventory, and navigating to the **Updates** tab. In the top-right corner, there is a pre-check remediation card from where you can generate the report.

From the vSphere Web Client, you can generate a pre-check remediation report when you create a remediation task for hosts that are contained in a cluster. You generate the report from the **Cluster Remediation Options** page of the **Remediate** wizard.

Table 9-2. Pre-Check Remediation Report for Clusters

Current Configuration/Issue	Recommended action	Details
Is DPM disabled?	Disable DPM on the cluster.	If a host has no running virtual machines, DPM might put the host in standby mode before or during remediation and Update Manager cannot remediate them. Disable DPM on a cluster to ensure that the remediation process is successful.
Is DRS enabled?	Enable DRS on the cluster.	DRS enables vCenter Server to place and migrate virtual machines automatically on hosts to attain the best use of cluster resources.
Is HA admission control disabled?	Disable HA admission control.	HA admission control prevents migration of the virtual machines with vMotion and the hosts cannot enter maintenance mode. Disable HA admission control on a cluster to make sure that remediation is successful.
Is EVC disabled on the cluster?	Enable EVC on the cluster.	EVC helps ensure vMotion compatibility between hosts in a cluster. When enabled on compatible hosts, EVC ensures that all hosts in a cluster present a common set of CPU features to virtual machines. EVC must be enabled so that the virtual machines are migrated successfully within the cluster during remediation.

Table 9-3. Pre-Check Remediation Report for Virtual Machines

Current Configuration/Issue	Changes applied for remediation	Details
A CD/DVD drive is attached.	Disconnect the CD/DVD drive.	Any CD/DVD drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
A floppy drive is attached.	Disconnect the floppy drive.	Any floppy drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
FT is enabled for a VM on a host in the cluster. FT prevents successful remediation.	Disable FT on the virtual machine.	If FT is enabled on for any of the virtual machines on a host, Update Manager cannot remediate that host.
VMware vCenter Server is installed on the virtual machine and DRS is disabled on the cluster.	Enable DRS on the cluster and ensure that virtual machines can be migrated with vMotion.	One of the virtual machines in the cluster runs the vCenter Server instance that you currently use. If you enable DRS on the cluster, vMotion can migrate the VM where vCenter Server runs to ensure that the remediation process of the hosts in the cluster is successful.
VMware vSphere Update Manager is installed on the virtual machine and DRS is disabled on the cluster.	Enable DRS on the cluster and ensure that virtual machines can be migrated with vMotion.	One of the virtual machines in the cluster runs the Update Manager instance that you currently use. If you enable DRS on the cluster, vMotion can migrate the VM where Update Manager runs to ensure that the remediation process of the hosts in the cluster is successful.

Remediating Virtual Machines

You can manually remediate virtual machines against the predefined individual VM baselines or a VM baseline group containing VMware Tools and VM Hardware upgrade baselines. You can also schedule a remediation operation at a time that is convenient for you.

To remediate multiple virtual machines, they must be in one container, such as a folder, vApp, or a datacenter. You must then attach a baseline group or a set of individual virtual machine baselines to the container.

With Update Manager you can remediate templates. A template is a master copy of a virtual machine that can be used to create and provision new virtual machines.

You can set up automatic upgrades of VMware Tools on power cycle for virtual machines. For more information, see Upgrade VMware Tools on Power Cycle.

Note Update Manager does not support virtual machine patch baselines.

If a host is connected to vCenter Server by using an IPv6 address, you cannot scan and remediate virtual machines that run on the host.

Rolling Back to a Previous Version

If remediation fails, you can roll back virtual machines and appliances to their previous state.

You can configure Update Manager to take snapshots of virtual machines and appliances and to keep them indefinitely or for a specific period of time. After the remediation is completed, you can validate the remediation and delete the snapshots if you do not need them.

Note When you upgrade VMware Tools on power cycle in selected virtual machines, Update Manager does not take a snapshot of the virtual machines before remediation and you cannot roll back. Update Manager does not take snapshots of fault tolerant virtual machines.

Remediate Virtual Machines

You can manually remediate virtual machines immediately, or can schedule a remediation at a time that is convenient for you.

You can perform an orchestrated upgrade by using a virtual machine baseline group. The VMware Tools upgrade baseline runs first, followed by the virtual machine hardware upgrade baseline.

Procedure

1 Connect the vSphere Web Client to a vCenter Server Appliance, or a vCenter Server system with which Update Manager is registered, and select **Home > vCenter Inventory Lists**.

2 Select **Home > VMs and Templates**.

3 From the inventory object navigator, select a virtual machine, and click the **Update Manager** tab.

4 Click **Remediate**.

  If you selected a container object, all virtual machines in the container are also remediated.

5 On the Select baselines page of the **Remediate** wizard, select the baseline group and upgrade baselines to apply.

6 Select the virtual machines that you want to remediate, and click **Next**.

7 On the Schedule page, specify a name and an optional description for the task.

  The time you set for the scheduled task is the time of the vCenter Server instance to which Update Manager is connected.

8 Enter specific times for powered on, powered off, or suspended virtual machines, or keep the selected option to **Run this action now** to begin the process immediately after you complete the wizard.

9 (Optional) Choose whether to upgrade VMware Tools on power cycle.

   This option is active only when you perform an upgrade against a single Upgrade VMware Tools to Match Host baseline. You can only enable VMware Tools upgrade on power cycle from the **Remediate** wizard, but you cannot disable it. You can disable the setting by clicking the **VMware Tools upgrade settings** button in the Update Manager Compliance view and deselecting the check box of a virtual machine in the **Edit VMware Tools upgrade settings** window.

10 (Optional) Specify the rollback options.

   This option is not available if you selected to upgrade VMware Tools on power cycle.

   a On the Rollback Options page of the **Remediate** wizard, select **Take a snapshot of the virtual machines before remediation to enable rollback**.

      A snapshot of the virtual machine is taken before remediation. If the virtual machine needs to roll back, you can revert to this snapshot.

      Update Manager does not take snapshots of fault tolerant virtual machines.

      If you perform a VMware Tools upgrade and select to upgrade VMware Tools on power cycle, Update Manager takes no snapshots of the selected virtual machines before remediation.

   b Specify when the snapshot should be deleted or select **Don't delete snapshots**.

   c Enter a name and optionally a description for the snapshot.

   d (Optional) Select the **Take a snapshot of the memory for the virtual machine** check box.

11 Click **Next**.

12 Review the Ready to Complete page, and click **Finish**.

Upgrade VMware Tools on Power Cycle

You can automate the process to upgrade VMware Tools for the virtual machines in your inventory.

You can set up Update Manager to perform a check of the VMware Tools version when a machine is powered on or restarted. If necessary, Update Manager upgrades VMware Tools to the latest version supported by the host that is running the virtual machine.

When you perform a VMware Tools upgrade on power cycle, Update Manager does not take a snapshot of the virtual machine, and you cannot roll back to the previous version.

Procedure

1 In the vSphere Web Client, select **Home > VMs and Templates**, and select a virtual machine or a folder.

2 Right-click a virtual machine or a folder and select **Update Manager > VMware Tools Upgrade Settings**

   The **Edit VMware Tools upgrade settings** wizard opens.

3 Select the virtual machines for which you want to enable VMware Tools upgrade on power cycle, and click **OK**.

The next time the virtual machines are restarted or powered on, Update Manager checks the version of VMware Tools installed in the machines and performs an upgrade, if necessary.

Scheduling Remediation for Hosts and Virtual Machines

You can schedule the remediation process of hosts and virtual machines by using the **Remediate** wizard.

You can schedule remediation for all hosts or all virtual machines in a container object from the vSphere inventory. You can perform scheduled orchestrated upgrades of the hosts or virtual machines in a selected container object.

To schedule remediation, you must specify a time for the remediation process on the Schedule page of the **Remediate** wizard.

vCenter Server uses the clock of the vCenter Server host machine for the tasks that you schedule. If you schedule to remediate an ESXi host that is in a different time zone from the vCenter Server instance, the scheduled time you see in the **Scheduled Tasks**, is the time of the vCenter Server time zone, and not time zone of the ESXi host. You can navigate to the **Scheduled Tasks** from the **Monitor** tab, under **Task & Events**.

You cannot edit existing scheduled remediation tasks. You can remove a scheduled remediation task and create a new one in its place.

If your vCenter Server system is connected to other vCenter Server by a common vCenter Single Sign-On domain, and you have installed and registered more than one Update Manager instance, you can create scheduled tasks for each vCenter Server instance. Scheduled tasks you create are specific only to the Update Manager instance you specify and are not propagated to the other instances in the group. From the navigation bar, you can specify an Update Manager instance by selecting the name of the vCenter Server system with which the Update Manager instance is registered.

View Update Manager Events 10

Update Manager stores data about events. You can review this event data to gather information about operations that are in progress or are completed.

Prerequisites

Connect thevSphere Web Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** icon.

Procedure

- In the Update Manager Administration view, click the **Events** tab to get information about recent events.

Update Manager Events

Update Manager displays events that help you monitor the processes that the system is completing.

Table 10-1. Update Manager Events

Type	Message Text	Action
Info	Successfully downloaded host patch definitions. New patches: *number_of_patches*.	
Error	Could not download host patch definitions.	Check your network connection to make sure that your metadata source is reachable.
Info	Successfully downloaded host patch packages. New packages: *number_of_packages*.	
Error	Could not download host patch packages.	Check your network connection to make sure that your patch source is reachable.
Info	Successfully downloaded notifications. New notifications: *number_of_notifications*.	
Error	Could not download notifications.	Check your network connection.
Info	Successfully scanned *vSphere_object_name*.	
Info	Scanning object *vSphere_object_name*.	
Error	Scanning of *vSphereHost* upgrade in progress: Migrating ESX v3 configuration to ESX v4 *vSphere_object_name* is canceled by user.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Could not scan *vSphere_object_name*.	Check the Update Manager log (`vmware-vum-server-log4cpp.log`) for scan errors.
Warning	Found a missing patch: *patch_name* when scanning *vSphere_object_name*. Re-downloading patch definitions might resolve this problem.	
Info	Successfully scanned *vSphere_object_name* for VMware Tools upgrades.	
Error	Could not scan *vSphere_object_name* for VMware Tools upgrades.	
Warning	VMware Tools is not installed on *vSphere_object_name*. VMware vSphere Update Manager supports upgrading only an existing VMware Tools installation.	
Warning	VMware Tools upgrade scan was not performed on *virtual_machine_name*. VMware Tools upgrade scan is supported only for VMs that run on ESXi 6.0 and later.	
Warning	VMware Tools upgrade was not performed on *virtual_machine_name*. VMware Tools upgrade is supported only for VMs that run on ESXi 6.0 and later.	
Error	Could not scan *virtual_machine_name* because the virtual machine has an invalid connection state: *virtual_machine_connection_state*.	Check the state of the virtual machine. Reboot the virtual machine to facilitate scanning.
Error	Could not scan *host_name* because the host has an invalid connection state: *host_connection_state*.	Check the state of the host. Reboot the host to facilitate scanning.
Info	Remediation succeeded for *vSphere_object_name*.	
Info	Remediating object *vSphere_object_name*.	
Error	Remediation did not succeed for *vSphere_object_name*.	Check the Update Manager log (`vmware-vum-server-log4cpp.log`) for remediation errors.
Info	VMware Tools upgrade succeeded for *vSphere_object_name*.	
Error	VMware Tools upgrade did not succeed for *vSphere_object_name*.	
Info	Successfully enabled the option for VMware Tools upgrade on VM power cycle for *virtual_machine_name*.	
Error	Could not enable the option for VMware Tools upgrade on VM power cycle for *virtual_machine_name*.	
Info	Successfully disabled the option for VMware Tools upgrade on VM power cycle for *virtual_machine_name*.	
Error	Could not disable the option for VMware Tools upgrade on VM power cycle for *virtual_machine_name*.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Could not remediate *virtual_machine_name* because the virtual machine has an invalid connection state: *virtual_machine_connection_state*.	Check the virtual machine's state. Restart the virtual machine to facilitate remediation.
Error	Could not remediate *host_name* because the host has an invalid connection state: *host_connection_state*.	Check the state of the host. Restart the host to facilitate remediation.
Info	Staging succeeded for *vSphere_object_name*.	
Error	Staging did not succeed for *vSphere_object_name*, *error_message*.	
Info	Staging patches to host *host_name*.	
Error	Could not stage patches to *host_name* because the host has an invalid connection state: *host_connection_state*.	
Error	Scan or remediation is not supported on *vSphere_object_name* because of unsupported or unknown OS: *operating_system_name*.	
Info	VMware vSphere Update Manager download alert (critical/total): ESX `data.esxCritical/data.esxTotal`.	Provides information about the number of patches downloaded.
Info	VMware vSphere Update Manager notification download alert	
Info	VMware vSphere Update Manager recall alert	
Info	VMware vSphere Update Manager recall fix alert	
Info	VMware vSphere Update Manager informative notification (moderate) alert	
Info	VMware vSphere Update Manager informative notification (important) alert	
Info	VMware vSphere Update Manager informative notification (critical) alert	
Error	Could not scan *virtual_machine_name* because host *host_name* is of unsupported version *host_version*.	For the latest information on which virtual machines can be scanned, see the release notes.
Error	Could not remediate *virtual_machine_name* because host *host_name* is of unsupported version *host_version*.	For the latest information on which hosts can be scanned, see the release notes.
Error	Could not scan *host_name* for patches because it is of unsupported version *host_version*.	For the latest information on which ESXi hosts can be scanned, see the release notes.
Error	Could not stage patches to *host_name* because it is of unsupported version *host_version*.	You can stage patches to hosts that are running ESXi 5.0 or later.
Error	Could not remediate *host_name* because it is of unsupported version *host_version*.	For the latest information on which ESXi hosts can be remediated, see the release notes.
Error	There is no VMware vSphere Update Manager license for *vSphere_object_name* for the required operation.	Obtain the required licenses to complete the desired task.

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	VMware vSphere Update Manager is running out of storage space. Location: *path_location*. Available space: *free_space*.	Add more storage.
Warning	VMware vSphere Update Manager is critically low on storage space! Location: *path_location*. Available space: *free_space*.	Add more storage.
Error	An unknown internal error occurred during the required operation on *virtual_machine_name*. Check the logs for more details and retry the operation.	
Error	Could not install patches on *vSphere_object_name*.	
Info	Installation of patches *patch_ID* started on host *host_name*.	
Info	Installation of patches *patch_ID* succeeded on *host_name*.	
Info	The following additional patches are included to resolve a conflict for installation on *vSphere_object_name*: *message*.	
Info	To resolve a conflict for installation on *vSphere_object_name*, the following additional patches might need to be included in the baseline: *message*.	
Info	VMware vSphere Update Manager could not find patches to resolve the conflict for installation on *vSphere_object_name*.	
Info	Installation of patches succeeded on *vSphere_object_name*.	
Info	Start rebooting host *host_name*.	
Info	Waiting for host *host_name* to reboot.	
Info	Host *host_name* is successfully rebooted.	
Error	Cannot reboot host *host_name*.	
Error	Cannot stage patch *patch_name* to *host_name*.	
Info	Staging of patch to *host_name* succeeded.	
Info	Started staging of patches *patch_IDs* on *host_name*.	
Info	Sysprep settings are restored.	
Info	Sysprep is disabled during the remediation.	
Info	Could not scan orphaned VM *virtual_machine_name*.	
Info	Could not remediate orphaned VM *virtual_machine_name*.	
Error	Could not download patch packages for following patches: *message*.	Check your network connections to make sure that your patch source is reachable.
Warning	*virtual_machine_name* contains an unsupported volume *volume_label*. Scan results for this VM might be incomplete.	
Info	Canceling task on *vSphere_object_name*.	
Warning	There are running tasks for the entity *vSphere_object_name* that cannot finish within a specific time. The operation will stop.	
Warning	Action is not supported for Linux VM *virtual_machine_name*. VMware Tools is not installed or the machine cannot start.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	Open *vSphere_object_name* firewall ports.	
Info	Close *vSphere_object_name* firewall ports.	
Info	Patch definitions for *vSphere_object_name* are missing. Download patch definitions first.	
Info	Patch definition for *vSphere_object_name* is corrupt. Check the logs for more details. Re-downloading patch definitions might resolve this problem.	
Info	Host upgrade in progress: Clearing partitions.	
Info	Host upgrade in progress: Partitioning physical hard drives.	
Info	Host upgrade in progress: Partitioning virtual hard drives.	
Info	Host upgrade in progress: Mounting file systems.	
Info	Host upgrade in progress: Installing packages.	
Info	Host upgrade in progress: Migrating ESXi v3 configuration to ESXi v4.	
Info	Host upgrade in progress: Installing network configuration.	
Info	Host upgrade in progress: Setting timezone.	
Info	Host upgrade in progress: Setting keyboard.	
Info	Host upgrade in progress: Setting language.	
Info	Host upgrade in progress: Configuring authentication.	
Info	Host upgrade in progress: Setting root password.	
Info	Host upgrade in progress: Boot setup.	
Info	Host upgrade in progress: Running postinstallation script.	
Info	Host upgrade installer completed.	
Error	Host upgrade installer stopped.	
Info	Host upgrade in progress.	
Error	Host version *host_version* is not supported for upgrade.	
Error	The host cannot be upgraded due to incompatible partition layout.	
Error	Upgrade requires at least *disk_size*MB free space on root partition, only *disk_size*MB found.	
Error	Upgrade requires at least *disk_size*MB free space on bootbank, only *disk_size*MB found.	
Error	Upgrade requires at least *disk_size*MB free space on VMFS datastore, only *disk_size*MB found.	
Warning	Insufficient memory found on the host: *memory_size*MB required, *memory_size*MB found.	
Error	Error in ESX configuration file *configuration_file*.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	The passwords cannot be migrated because the password encryption scheme is incompatible.	
Warning	Unsupported devices found on the host.	
Warning	The software modules *modules* found on the host are not part of the upgrade image. These modules will be removed during upgrade.	
Warning	Cisco Nexus 1000v vNetwork Distributed Switch feature installed on the host will be removed during upgrade.	
Warning	Cisco Nexus 1000v vNetwork Distributed Switch software package *package_name* in the upgrade image is incompatible with the Cisco Nexus 1000v software package *package_name* installed on the host. Upgrading the host will remove the feature from the host.	
Warning	There is no Cisco Nexus 1000v vNetwork Distributed Switch software package in the upgrade image. Upgrading the host will remove the feature from the host.	
Warning	Cisco Nexus 1000v vNetwork Distributed Switch software package *package_name* in the upgrade image is incompatible with the Cisco Nexus 1000v VSM managing the vDS. Upgrading the host will remove the feature from the host.	
Warning	There is no Cisco Nexus 1000v vNetwork Distributed Switch software package in the upgrade image that is compatible with the Cisco Nexus 1000v VSM managing the vDS. Upgrading the host will remove the feature from the host.	
Warning	EMC PowerPath module *module* installed on the host will be removed during upgrade.	
Error	Upgrade precheck script error.	
Info	Successfully scanned *vSphere_object_name* for Virtual Hardware upgrades.	
Error	Could not scan *vSphere_object_name* for Virtual Hardware upgrades.	
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools is not the latest version. To upgrade virtual hardware, VMware Tools must be the latest version.	
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools state is unknown. To upgrade virtual hardware, VMware Tools must be the latest version.	
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools is not installed. To upgrade virtual hardware, VMware Tools must be the latest version.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools state is not managed by VMware vSphere. To upgrade virtual hardware, VMware Tools must be the latest version.	
Warning	Virtual Hardware upgrade scan was not performed for *virtual_machine_name*. Virtual Hardware upgrade scan is supported only for VMs that run on ESXi 6.0 hosts and later.	
Warning	Virtual Hardware upgrade was not performed for *virtual_machine_name*. Virtual Hardware upgrade is supported only for VMs that run on ESXi 6.0 and later.	
Info	Virtual Hardware upgrade succeeded for *vSphere_object_name*.	
Error	Could not perform Virtual Hardware upgrade on *vSphere_object_name*.	
Error	VM *virtual_machine_name* has either VMware vSphere Update Manager or VMware vCenter Server installed. This VM will be ignored for scan and remediation.	Virtual machines on which Update Manager or vCenter Server is installed are not scanned or remediated.
Error	The host *host_name* has a VM *virtual_machine_name* with VMware vSphere Update Manager or VMware vCenter Server installed. The VM must be moved to another host for the remediation to proceed.	If a virtual machine on which Update Manager or vCenter Server is installed is on a host that is going to be remediated, the virtual machine is migrated to another host.
Error	Error while waiting for VMware Tools to respond. Verify that VMware Tools is running in VM *virtual_machine_name*.	
Error	The version of VMware Tools installed in *virtual_machine_name* does not support automatic upgrade. Upgrade VMware Tools manually.	
Info	Suspended VM *virtual_machine_name* has been skipped.	
Warning	Cannot remediate host *host_name* because it is a part of a VMware DPM enabled cluster.	Update Manager does not remediate hosts in clusters with enabled VMware DPM. Disable VMware DPM.
Warning	Cannot scan host *host_name* because it is a part of a VMware DPM enabled cluster.	Update Manager does not scan hosts in clusters with enabled VMware DPM. Disable VMware DPM.
Warning	Cannot stage host *host_name* because it is a part of a VMware DPM enabled cluster.	Update Manager does not stage patches to hosts in clusters with enabled VMware DPM. Disable VMware DPM.
Warning	Cannot remediate host *host_name* because it is a part of a HA admission control enabled cluster.	Update Manager does not remediate hosts in clusters with enabled HA admission control. Disable HA admission control.
Warning	Cannot remediate host *host_name* because it contains one or more Primary or Secondary VMs on which FT is enabled.	Update Manager does not remediate hosts in clusters on which virtual machines are with enabled FT. Disable FT.

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	Cannot remediate host *host_name* because it is a part of a VMware DPM enabled cluster and contains one or more Primary or Secondary VMs on which FT is enabled.	Update Manager does not remediate hosts in clusters with enabled VMware DPM and hosts on which virtual machines are with enabled FT. Disable VMware DPM and FT.
Warning	Host *host_name* has FT enabled VMs. If you apply different patches to hosts in a cluster, FT cannot be re-enabled.	Update Manager does not remediate hosts in clusters on which virtual machines are with enabled FT. Disable FT.
Warning	Host *host_name* has FT enabled VMs. The host on which the Secondary VMs reside is not selected for remediation. As a result FT cannot be re-enabled.	Update Manager does not remediate hosts in clusters on which virtual machines are with enabled FT. Disable FT.
Warning	Host *host_name* is a PXE booted ESXi host. Scanning, staging, and remediation are not supported on PXE booted ESXi hosts of version 4.x.	
Warning	Host *host_name* is a PXE booted ESXi 5.0 host. You did not enable remediation of this host.	You can enable remediation for PXE booted ESXi hosts of version 5.0.
Warning	Cannot remediate host *host_name* because it has VMs with a connected removable device. Disconnect all removable devices before remediation.	Update Manager does not remediate hosts in clusters on which the virtual machines are with connected removable devices such as CD/DVD or floppy drives. Disconnect any removable devices from the virtual machines on a host.
Error	Cannot remediate host *host_name* because it cannot enter maintenance mode.	
Error	Cannot remediate host *host_name* because it cannot enter maintenance mode *reason*.	
Error	Cannot migrate VM *virtual_machine_name* from *source_host_name* to *destination_host_name*.	If virtual machines cannot be migrated with vMotion, and the host cannot enter maintenance mode, Update Manager does not remediate the host.
Error	Cannot enable FT for VM *virtual_machine_name* on host *host_name*.	
Error	Cannot disable FT for VM *virtual_machine_name* on host *host_name*.	Update Manager does not scan, stage, or remediate hosts on which virtual machines are with enabled FT.
Error	Cannot check compatibility of the VM *virtual_machine_name* for migration with vMotion to host *host_name*.	
Error	VMware vSphere Update Manager could not restore HA admission control/DPM settings for cluster *cluster_name* to their original values. These settings have been changed for patch installation. Check the cluster settings and restore them manually.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	VMware vSphere Update Manager could not restore initial Fault Tolerance state of one or more virtual machines. Check the Fault Tolerance settings and restore them manually.	
Error	VMware vSphere Update Manager could not restore the original power state for all VMs in cluster *cluster_name*. These settings have been changed for patch installation. You can manually restore the original power state of the VMs.	
Error	VMware vSphere Update Manager could not restore the original removable device connection settings for all VMs in cluster *cluster_name*. These settings have been changed for patch installation. You can manually restore the settings for the VMs.	
Error	Cannot deploy upgrade agent on host.	
Error	Unable to verify host reboot. To complete the upgrade reboot the host *host_name* manually.	Reboot the host.
Error	Cannot run upgrade script on host.	
Error	Host patch *patch_name* conflicts with patch *patch_name* included in the baseline and cannot be staged. Remove either of the patch from the baseline and retry the stage operation.	Remove one of the conflicting patches and retry the stage operation.
Error	Host patch *patch_name* conflicts with the package *package_name* installed on the host and cannot be staged. Remove the patch from the baseline or include any suggested additional patches in the baseline and retry stage operation.	Remove the conflicting patch from the baseline and retry the stage
Error	Host patch *patch_name* conflicts with patch *patch_name* included in the baseline and cannot be remediated. Remove either of the patch from the baseline and retry the remediation.	Remove one of the conflicting patches from the baseline and retry the remediation.
Error	Host patch *patch_name* conflicts with the package *package_name* installed on the host and cannot be remediated. Remove the patch from the baseline or include any suggested additional patches in the baseline and retry remediation operation.	Remove the conflicting patch from the baseline and retry the remediation.
Info	Package *package_name* is successfully imported.	
Error	Import of package: *package_name* did not succeed.	
Info	*number_bulletins* new bulletins uploaded successfully through offline bundle.	
Error	Host patch offline bundle upload did not succeed.	
Info	Host patch offline bundle upload is canceled by user.	
Info	Scanning, remediation, and staging are not supported on PXE booted ESXi hosts.	
Error	Cannot remediate the host because the removable devices cannot be disconnected from the VMs that are running on the host.	
Error	PXE booted ESXi host *host_name* is supported for staging and remediation.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	Patch *patch_name* was excluded from the stage operation because its prerequisite *prerequisite_name* is neither installed on the host nor included in the baseline. Include the prerequisites in a Patch or Extension baseline and retry the stage operation. You can also add the baselines to a baseline group for convenience and perform the stage operation.	Include the prerequisites in a Patch or Extension baseline and retry the stage operation.
Warning	Patch *patch_name* was excluded from the remediation because its prerequisite *prerequisite_name* is neither installed on the host nor included in the baseline. Include the prerequisites in a Patch or Extension baseline and retry the remediation. You can also add the baselines to a baseline group for convenience and perform the remediation.	Include the prerequisites in a Patch or Extension baseline and retry the stage operation.
Error	Cannot scan the host *host_name* because its power state is *state*.	
Error	Cannot stage patches to the host *host_name* because its power state is *state*.	
Error	Cannot remediate the host *host_name* because its power state is *state*.	
Error	Could not scan host *host_name* because its power state is invalid. The host is in standby mode and the individual VMware DPM settings of the host are set to Disabled or Manual.	Power on the host manually.
Error	Could not stage patches to host *host_name* because its power state is invalid. The host is in standby mode and the individual VMware DPM settings of the host are set to Disabled or Manual.	Power on the host manually.
Error	Could not remediate host *host_name* because its power state is invalid. The host is in standby mode and the individual VMware DPM settings of the host are set to Disabled or Manual.	Power on the host manually.
Info	Scanning PXE booted ESXi host *host_name*.	
Warning	Staging patches to PXE booted ESXi host *host_name*. If the host is rebooted prior to remediation of the staged patches, these patches will no longer remain staged and will be lost.	
Warning	Remediating PXE booted ESXi host *host_name*. If the host is rebooted prior to updating the image profile associated with the host, the applied patches will longer remain installed and will be lost.	
Warning	Staging patches whose installation requires a host reboot is not supported on PXE booted ESXi host *host_name*. Update your image profile.	
Warning	Remediation of PXE booted ESXi host *host_name* against patches that require a host reboot is not supported. Remove these patches from the baseline to install the patches that do not require a reboot. To install patches requiring a reboot, update your image profile.	

Table 10-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Host *host_name* cannot download files from the VMware vSphere Update Manager patch store. Check the network connectivity and firewall setup, and verify that the host can access the configured patch store.	
Error	Remediation did not succeed for *host_name*. The host could not enter maintenance mode.	
Error	Remediation did not succeed for *host_name*. The host could not exit maintenance mode.	
Error	Remediation did not succeed for *host_name*. The host did not reboot after remediation.	
Error	Remediation did not succeed for *host_name*. VMware vSphere Update Manager timed out waiting for the host to reconnect.	
Error	Remediation did not succeed for *host_name*. VMware vSphere Update Manager timed out waiting for the host to reconnect after a reboot.	
Error	Remediation did not succeed for *host_name*. Restoring the power state or device connection state for one or more virtual machines on the host did not succeed.	
Error	Remediation did not succeed for *host_name*. The patch metadata is corrupted. This might be caused by an invalid format of metadata content. You can try to re-download the patches.	
Error	Remediation did not succeed for *host_name*. There were errors while downloading one or more software packages. Check the VMware vSphere Update Manager network connectivity settings.	
Error	Remediation did not succeed for *host_name*. The host has virtual machines *machine* with connected removable media devices. This prevents the host from entering maintenance mode. Disconnect the removable devices and try again.	
Error	The patches selected for remediation on the host *host_name* depend on other patches that have conflicts.	
Error	Remediation did not succeed for *host_name*.	

The Update Manager Patch Repository 11

Update Manager stores patch and extension metadata.

You can use the patch repository for various tasks, such as the following:

- Manage patches and extensions
- Check for new patches and extensions
- View patch and extension details
- View the baselines in which a patch or an extension is included
- View recalled patches
- Import patches

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, and you have at least one Update Manager instance, you can select the Update Manager repository that you want to view.

In the vSphere Web Client, you can find the patch repository in the Update Manager Admin view, where under the **Manage** tab there is a **Patch Repository** tab.

In the vSphere Client, the patch repository is available from the Update Manager Home view under the **Updates** tab.

Add or Remove Patches From a Baseline

You can edit the content of a custom patch baselines from the Update Manager Admin view.

Prerequisites

Required privileges: **VMware vSphere Update Manager.Manage Baselines**

Procedure

1 In the Home view of the vSphere Web Client, select the Update Manager icon.

2 From the **Objects** tab, select an Update Manager instance.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

3 Click the **Manage** tab, and click **Patch Repository**.

4 Select a patch from the list, and click **Add to baseline**.

   The Edit containing baselines dialog box opens.

5 Select the baselines in which you want to include the patch.

   - To add the patch to a baseline, select that baseline from the list.
   - To remove the patch from a baseline, deselect the baseline from the list.

   Note Do not deselect an already selected baseline, unless you want to remove the patch from that baseline.

6 Click **OK**.

Troubleshooting 12

If you encounter problems when running or using Update Manager, you can use a troubleshooting topic to understand and solve the problem, if there is a workaround.

This chapter includes the following topics:

- Update Manager Client Interface Remains Visible in the vSphere Web Client After Uninstalling Update Manager Server
- Connection Loss with Update Manager Server or vCenter Server in a Single vCenter Server System
- Gather Update Manager Log Bundles
- Gather Update Manager and vCenter Server Log Bundles
- Log Bundle Is Not Generated
- Host Extension Remediation or Staging Fails Due to Missing Prerequisites
- No Baseline Updates Available
- All Updates in Compliance Reports Are Displayed as Not Applicable
- All Updates in Compliance Reports Are Unknown
- VMware Tools Upgrade Fails if VMware Tools Is Not Installed
- ESXi Host Scanning Fails
- ESXi Host Upgrade Fails
- The Update Manager Repository Cannot Be Deleted
- Incompatible Compliance State

Update Manager Client Interface Remains Visible in the vSphere Web Client After Uninstalling Update Manager Server

After you uninstall Update Manager server, the **Update Manager** tab might remain visible in the vSphere Web Client.

Problem

The **Scan** and **Attach** buttons appear active, but if you click them, the following error message appears:

```
There was an error connecting to VMware vSphere Update Manager.
```

Also after uninstalling the Update Manager server, the Update Manager installation directory might still contain files. This does not affect future installations of Update Manager.

Solution

- Log out and log in to the vSphere Web Client.

  The **Update Manager** tab disappears from the vSphere Web Client.

Connection Loss with Update Manager Server or vCenter Server in a Single vCenter Server System

Because of loss of network connectivity or the restart of the servers, the connection between the Update Manager plug-in and the Update Manager server or vCenter Server system might get interrupted.

Problem

The connection between the Update Manager Client plug-in and the Update Manager server or vCenter Server system is interrupted, when the servers are restarting or are stopped. In such a case various symptoms are observed.

- Update Manager Client plug-in displays a reconnection dialog, and after 15-20 seconds, a failure message appears. The plug-in is disabled.
- Update Manager Client plug-in displays a reconnection dialog. Within 15-20 seconds, the dialog disappears, and the Client plug-in can be used.
- vSphere Client displays a reconnection dialog. After an interval, it displays the login form.

Cause

- The Update Manager server stops and is not available for more than 15-20 seconds.
- The Update Manager server restarts, and the service becomes available within 15-20 seconds.
- vCenter Server stops.

Solution

- If the Update Manager server has stopped, start the Update Manager service and re-enable the Update Manager Client plug-in.
- If the Update Manager server has restarted, wait for it to become available.
- If the vCenter Server service has stopped, start the vCenter Server service and enable the Update Manager Client plug-in.

Gather Update Manager Log Bundles

You can gather information about recent events on the Update Manager server for diagnostic purposes.

Procedure

1 Log in to the machine on which Update Manager is installed.

   To obtain the complete set of the logs, log in with the user name and password used for installing Update Manager.

2 Generate the Update Manager log bundle.

   - For Microsoft Windows Server 2008, select **Start > All Programs > VMware > Generate Update Manager log bundle**.
   - For Microsoft Windows Server 2012, click **Start**, enter **Generate Update Manager log bundle**, and press Enter.

Log files are generated as a ZIP package, which is stored on the current user's desktop.

Gather Update Manager and vCenter Server Log Bundles

When the Update Manager server and vCenter Server are installed on the same computer, you can gather information about recent events on the Update Manager server and vCenter Server system for diagnostic purposes.

Procedure

1 Log in as an administrator to the computer on which vCenter Server and Update Manager are installed.

2 Generate the vCenter Server log bundle.

   - For Microsoft Windows Server 2008, select **Start > All Programs > VMware > Generate vCenter Server log bundle**.
   - For Microsoft Windows Server 2012, click **Start**, enter **Generate vCenter Server log bundle**, and click **Entrer**.

3 Generate the Update Manager log bundle.

   - For Microsoft Windows Server 2008, select **Start > All Programs > VMware > Generate Update Manager log bundle**.
   - For Microsoft Windows Server 2012, click **Start**, enter **Generate Update Manager log bundle**, and press Enter.

Log files for vCenter Server and Update Manager are generated as a ZIP package, which is stored on the current user's desktop.

Log Bundle Is Not Generated

Although the script seems to complete successfully, an Update Manager log bundle might not be generated. Because of limitations in the ZIP utility that Update Manager uses, the cumulative log bundle size cannot exceed 2 GB. If the log exceeds 2 GB, the operation might fail.

Problem

Update Manager does not generate log bundle after you run the script.

Solution

1 Log in to the machine where Update Manager runs, and open a Command Prompt window.

2 Change to the directory where Update Manager is installed.

   The default location is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 To run the script, and exclude the vCenter Server logs, enter the following command:

   `cscript vum-support.wsf /n`

   The **`/n`** option lets the script to skip the vCenter Server support bundle and collect only the Update Manager log bundle.

4 Press Enter.

   The Update Manager log bundle is generated as a ZIP package successfully.

Host Extension Remediation or Staging Fails Due to Missing Prerequisites

Some host extension remediation or staging operations fail because Update Manager does not automatically download and install missing prerequisites.

Problem

Host extension remediation or staging might fail.

Cause

Update Manager skips the extensions with missing prerequisites and lists the missing prerequisites as events when it detects them during the staging and remediation operations. To proceed with staging and remediation, you must install the prerequisites.

Solution

1 To see which prerequisites are missing, in Compliance View select **Tasks & Events > Events**.

2 Add the missing prerequisites manually to either an extension or a patch baseline, depending on the type of the missing prerequisites.

3 (Optional) Create a baseline group that contains the new baseline as well as the original baseline.

4 Remediate the host against the two baselines.

No Baseline Updates Available

Baselines are based on metadata that Update Manager downloads from the VMware and third-party websites.

Problem

Updates for ESXi hosts might be unavailable.

Cause

- Misconfigured Web server proxy.
- Third-party servers are unavailable.
- VMware update service is unavailable.
- Poor network connectivity.

Solution

- Check the connectivity settings. For more information, see Change the Update Manager Network Settings.
- Check the third-party websites to determine whether they are available.
- Check the VMware website (http://www.vmware.com) to determine whether it is available.
- Check whether other applications that use networking are functioning as expected. Consult your network administrator whether the network is working as expected.

All Updates in Compliance Reports Are Displayed as Not Applicable

Scan results usually consist of a mix of installed, missing, and not applicable results. Not applicable entries are only a concern when this is the universal result or when you know that the patches should be applicable.

Problem

A scan might result in all baselines being marked as Not Applicable.

Cause

This condition typically indicates an error in scanning.

Solution

1 Examine the server logs for scan tasks that are marked as failed.

2 Retry the scan operation.

All Updates in Compliance Reports Are Unknown

Scanning is the process in which you generate compliance information about vSphere objects against attached baselines and baseline groups. The compliance statuses of objects can be All Applicable, Non Compliant, Incompatible, Unknown, and Compliant.

Problem

All results of a scan might be listed as Unknown.

Cause

Such a condition typically indicates an error at the start of the scanning process. This might also indicate that no scan occurred or that the object is not supported for scan.

Solution

Schedule a scan or manually start a scan.

VMware Tools Upgrade Fails if VMware Tools Is Not Installed

Update Manager upgrades only an existing installation of VMware Tools in a virtual machine running on a host of version ESXi 5.x or later.

Problem

You cannot upgrade VMware Tools because a virtual machine in incompatible compliance state cannot be remediated.

Cause

If no VMware Tools installation is detected on a virtual machine, a scan of the virtual machine against the VMware Tools Upgrade to Match Host baseline or a baseline group containing this baseline results in an incompatible compliance state of the virtual machine.

Solution

Install VMware Tools manually, or right-click the virtual machine, and select **Guest > Install/Upgrade VMware Tools**.

ESXi Host Scanning Fails

Scanning is the process in which you generate compliance information about the vSphere objects against attached baselines and baseline groups. In some cases, the scan of ESXi hosts might fail.

Problem

The scan process of ESXi hosts might fail.

Cause

If the VMware vSphere Update Manager Update Download task is not completed successfully after you add a host to the vSphere inventory, no host patch metadata is downloaded.

Solution

After you add a host or a virtual machine to the vSphere inventory, run the VMware vSphere Update Manager Update Download task before performing the scan. For more information, see Run the VMware vSphere Update Manager Update Download Task.

ESXi Host Upgrade Fails

The remediation process of an ESXi host against an upgrade baseline or a baseline group containing an upgrade baseline might fail.

Problem

An ESXi host might fail to upgrade.

Cause

When you upgrade an ESXi host with less than 10MB of free space in its `/tmp` directory, although Update Manager indicates that the remediation process completed successfully, the ESXi host is not upgraded.

Solution

1. If you see an Agent Deploy failure, make sure that the `/tmp` directory has at least 10MB of free space.
2. Repeat the remediation process to upgrade the host.

The Update Manager Repository Cannot Be Deleted

When you uninstall the Update Manager server, you might want to delete the Update Manager repository.

Problem

You might not be able to delete the Update Manager repository.

Cause

The maximum number of characters that a filename (including the path) can contain on the operating system is set to 255 by default.

As part of the patch and upgrade download process, the files that Update Manager downloads in the Update Manager repository, might have paths that are deeper than the Windows *MAX_PATH*. You cannot open, edit, or delete such files, by using Windows Explorer, for example.

Map a network drive to a folder that is as deep in the folder tree of the Update Manager repository as possible. This shortens the virtual path.

Important Ensure that you have the necessary permissions on the network drive and the Update Manager repository. Otherwise, you might not be able to delete the files from the Update Manager repository.

Solution

- Map the local folder to a network drive, in a command prompt run the following command.

  ```
  subst Z: C:\Documents And Settings\All Users\Application Data\VMware\VMware Update
  Manager\data\vaupgrade\
  ```

  For example, if the path to the folder of the Update Manager repository where Update Manager stores virtual appliance upgrades is the following: `C:\Documents And Settings\All Users\Application Data\VMware\VMware Update Manager\data\vaupgrade\...` , and the total length of this path exceeds 255 characters, you should map a network drive to the `vaupgrade` directory (inclusive) or a directory deeper.

Incompatible Compliance State

After you perform a scan, the compliance state of the attached baseline might be incompatible. The incompatible compliance state requires more attention and further action to be resolved.

Incompatibility might be caused by an update in the baseline for a number of reasons.

Conflict The update conflicts with either an existing update on the host or another update in the Update Manager patch repository. Update Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform scan, remediation, and staging operations. In most cases, you can take action to resolve the conflict.

Conflicting New Module The host update is a new module that provides software for the first time, but is in conflict with either an existing update on the host or another update in the Update Manager repository. Update Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform scan, remediation, and staging operations. In most cases, you must take action to resolve the conflict.

Missing Package This state occurs when metadata for the update is in the depot but the corresponding binary payload is missing. The reasons can be that the product might not have an update for a given locale; the Update Manager patch repository is deleted or corrupt, and Update Manager no longer has Internet access to download updates; or you have manually deleted an upgrade package from the Update Manager repository.

Not Installable	The update cannot be installed. The scan operation might succeed on the target object, but remediation cannot be performed.
Incompatible Hardware	The hardware of the selected object is incompatible or has insufficient resources to support the update. For example, when you perform a host upgrade scan against a 32-bit host or if a host has insufficient RAM.
Unsupported Upgrade	The upgrade path is not possible. For example, the current hardware version of the virtual machine is greater than the highest version supported on the host.

Updates Are in Conflict or Conflicting New Module State

After you perform a successful scan, the compliance state of the attached baseline might be incompatible because of conflicting updates. The status of the update will be Conflict if the update is a patch, and Conflicting New Module, if the update is a new module.

Problem

The state of the attached baseline is incompatible because an update in the baseline is in conflict with either other updates in the Update Manager patch repository or an existing update on the host.

Cause

- The baseline contains a host update that conflicts with another update already installed on the host.
- The baseline contains a host update that conflicts with other updates in the Update Manager repository.
- The dynamic baseline criteria results in a conflicting set.
- The baseline is attached to a container object and conflicts with one or more inventory objects in the folder. This is an indirect conflict.

Solution

- Detach or remove the baseline containing the update that conflicts with another update already installed on the host.

  If Update Manager suggests a resolution for the conflicting update, add the resolution update into the baseline and retry the scan operation.
- Open the **Patch Details** or the **Extension Details** window to see details about the conflict and the other updates with which the selected update is in conflict.
  - If the conflicting updates are in the same baseline, remove the conflicting updates from the baseline and perform the scan again.
  - If the conflicting updates are not in the same baseline, ignore the conflict and proceed to install the updates by starting a remediation.

- Edit the dynamic baseline criteria or exclude the conflicting patches and scan again.

  If Update Manager suggests a resolution for the conflicting patch, add the resolution patches into the baseline and retry the scan operation.
- If the conflict is indirect, you can remediate the container object, but only the objects that are not in conflict are remediated. You should resolve the conflicts or move the inventory objects that are in conflict, and then remediate.

Updates Are in Missing Package State

The compliance state of the attached baseline might be incompatible because packages might be missing from updates.

Problem

When you perform a host upgrade scan, if the binary package for the host is missing or not uploaded, or if you upload the wrong binary package, the scan fails.

Solution

1. Edit the host upgrade baseline and import the required package.
2. Repeat the scan.

Updates Are in Not Installable State

After you perform a scan, the compliance state of the attached baseline might be displayed as incompatible because of updates that cannot be installed on the object.

Problem

The state of the attached baseline is incompatible because it contains updates that cannot be installed.

Cause

- A VMware Tools Upgrade to Match Host baseline is attached to a virtual machine on which VMware Tools is not installed. The **Upgrade Details** window shows the actual reason for the Incompatible state.
- A VMware Tools Upgrade to Match Host baseline is attached to a virtual machine with VMware Tools not managed by the VMware vSphere platform. The **Upgrade Details** window shows the actual reason for the Incompatible state.

Solution

- If VMware Tools is not installed on the virtual machine, install a version of VMware Tools and retry the scan operation.
- If VMware Tools on the virtual machine is not managed by the VMware vSphere platform, you should detach the baseline and perform the upgrade manually. For more information about upgrading VMware Tools when it is packaged and distributed as OSPs, see *VMware Tools Installation Guide for Operating System Specific Packages*.

Updates Are in Unsupported Upgrade State

After you perform a successful scan, the compliance state of the attached baseline might be incompatible because of unsupported upgrade.

Problem

The state of the attached baseline is incompatible because of an unsupported upgrade.

Cause

The upgrade path for the virtual hardware of the virtual machine is not possible, because the current hardware version is higher than the latest version supported on the host. The **Upgrade Details** window shows the actual hardware version.

Solution

No workaround is available. See the upgrade details to check the current hardware version.

13 Database Views

Update Manager uses Microsoft SQL Server and Oracle databases to store information. The database views for Microsoft SQL Server and Oracle databases are the same.

This chapter includes the following topics:

VUMV_VERSION

This database view contains Update Manager version information.

Table 13-1. VUMV_VERSION

Field	Notes
VERSION	Update Manager version in x.y.z format, for example 1.0.0
DATABASE_SCHEMA_VERSION	Update Manager database schema version (an increasing integer value), for example 1

VUMV_UPDATES

This database view contains software update metadata.

Table 13-2. VUMV_UPDATES

Field	Notes
UPDATE_ID	Unique ID generated by Update Manager
TYPE	Entity type: virtual machine or host
TITLE	Title
DESCRIPTION	Description
META_UID	Unique ID provided by the vendor for this update (for example, MS12444 for Microsoft updates)
SEVERITY	Update severity information: Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
RELEASE_DATE	Date on which this update was released by the vendor
DOWNLOAD_TIME	Date and time this update was downloaded by the Update Manager server into the Update Manager database
SPECIAL_ATTRIBUTE	Any special attribute associated with this update (for example, all Microsoft Service packs are marked as Service Pack)
COMPONENT	Target component, such as HOST_GENERAL, VM_GENERAL, VM_TOOLS, or VM_HARDWAREVERSION
UPDATECATEGORY	Specifies whether the update is a patch or an upgrade.

VUMV_HOST_UPGRADES

This database view provides detailed information about the host upgrade packages.

Table 13-3. VUMV_HOST_UPGRADES

Field	Notes
RELEASE_ID	Database-generated ID, which refers to VUMV_UPDATES and UPDATE_ID
PRODUCT	ESXi host
VERSION	Version number represented in x.y.z format
BUILD_NUMBER	Build number of the ESXi host version

Table 13-3. VUMV_HOST_UPGRADES (Continued)

Field	Notes
DISPLAY_NAME	Name displayed to the user
FILE_NAME	Name of the upgrade file

VUMV_PATCHES

This database view contains patch binary metadata.

Table 13-4. VUMV_PATCHES

Field	Notes
DOWNLOAD_URL	URL for the patch binary
PATCH_ID	Unique ID for the current patch, generated by the Update Manager server
TYPE	Patch type: virtual machine or host
NAME	Name of the patch
DOWNLOAD_TIME	Date and time the patch was downloaded by the Update Manager server into the Update Manager database
PATCH_SIZE	Size of the patch in KB

VUMV_BASELINES

This database view contains the details for a particular Update Manager baseline.

Table 13-5. VUMV_BASELINES

Field	Notes
BASELINE_ID	Unique ID generated for this baseline by the Update Manager server
NAME	Name of the baseline
BASELINE_VERSION	History of when the baseline has been changed (old version remains in the database)
TYPE	Baseline type: virtual machine or host
BASELINE_UPDATE_TYPE	Baseline type: fixed or dynamic
TARGET_COMPONENT	Target component, such as HOST_GENERAL, VM_GENERAL, VM_TOOLS, or VM_HARDWAREVERSION
BASELINE_CATEGORY	Baseline category, such as patch or upgrade

VUMV_BASELINE_GROUPS

This database view contains the details for a particular Update Manager baseline group.

Table 13-6. VUMV_BASELINE_GROUPS

Field	Notes
BASELINE_GROUP_ID	Unique ID generated for this baseline group by the Update Manager server
VERSION	Version of the baseline group
NAME	Name of the baseline group
TYPE	Type of targets that this baseline applies to: virtual machine or ESXi host
DESCRIPTION	Description of the baseline group
DELETED	Information about the baseline group deletion, if it is deleted
LASTUPDATED	Information about the last time that the baseline group was updated

VUMV_BASELINE_GROUP_MEMBERS

This database view contains information about the relationship between the baseline and the baseline group in which it is included.

Table 13-7. VUMV_BASELINE_GROUP_MEMBERS

Field	Notes
BASELINE_GROUP_ID	Unique ID generated for this baseline group by the Update Manager server
BASELINE_GROUP_VERSION	Version of the baseline group
BASELINE_ID	Name of the baseline included in the baseline group

VUMV_PRODUCTS

This database view contains product metadata, including that for operating systems and applications.

Table 13-8. VUMV_PRODUCTS

Field	Notes
PRODUCT_ID	Unique ID for the product, generated by the Update Manager server
NAME	Name of the product
VERSION	Product version
FAMILY	Windows, Linux, ESX host, or Embedded ESXi host, Installable ESXi host

VUMV_BASELINE_ENTITY

This database view contains the objects to which a particular baseline is attached.

Table 13-9. VUMV_BASELINE_ENTITY

Field	Notes
BASELINE_ID	Baseline ID (foreign key, VUMV_BASELINES)
ENTITY_UID	Unique ID of the entity (managed object ID generated by vCenter Server)

VUMV_UPDATE_PATCHES

This database view contains patch binaries that correspond to a software update.

Table 13-10. VUMV_UPDATE_PATCHES

Field	Notes
UPDATE_ID	Software update ID (foreign key, VUMV_UPDATES)
PATCH_ID	Patch ID (foreign key, VUMV_PATCHES)

VUMV_UPDATE_PRODUCT

This database view contains products (operating systems and applications) to which a particular software update is applicable.

Table 13-11. VUMV_UPDATE_PRODUCT

Field	Notes
UPDATE_ID	Software update ID (foreign key, VUMV_UPDATES)
PRODUCT_ID	Product ID (foreign key, VUMV_PRODUCTS)

VUMV_ENTITY_SCAN_HISTORY

This database view contains the history of scan operations.

Table 13-12. VUMV_ENTITY_SCAN_HISTORY

Field	Notes
SCAN_ID	Unique ID generated by the Update Manager server
ENTITY_UID	Unique ID of the entity the scan was initiated on
START_TIME	Start time of the scan operation
END_TIME	End time of the scan operation
SCAN_STATUS	Result of the scan operation (for example, Success, Failure, or Canceled)
FAILURE_REASON	Error message describing the reason for failure
SCAN_TYPE	Type of scan: patch or upgrade
TARGET_COMPONENT	Target component, such as HOST_GENERAL, VM_GENERAL, VM_TOOLS, or VM_HARDWAREVERSION

VUMV_ENTITY_REMEDIATION_HIST

This database view contains the history of remediation operations.

Table 13-13. VUMV_ENTITY_REMEDIATION_HIST

Field	Notes
REMEDIATION_ID	Unique ID generated by the Update Manager server
ENTITY_UID	Unique ID of the entity that the remediation was initiated on
START_TIME	Start time of the remediation
END_TIME	End time of the remediation
REMEDIATION_STATUS	Result of the remediation operation (for example, Success, Failure, or Canceled)
IS_SNAPSHOT_TAKEN	Indicates whether a snapshot was created before the remediation

VUMV_UPDATE_PRODUCT_DETAILS

This database view contains information about the products (operating systems and applications) to which a particular software update is applicable.

Table 13-14. VUMV_UPDATE_PRODUCT_DETAILS

Field	Notes
UPDATE_METAUID	Software update ID (foreign key, VUMV_UPDATES)
UPDATE_TITLE	Update title
UPDATE_SEVERITY	Update impact information: Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
PRODUCT_NAME	Product name
PRODUCT_VERSION	Product version

VUMV_BASELINE_UPDATE_DETAILS

This database view contains information about the software updates that are part of a baseline.

Table 13-15. VUMV_BASELINE_UPDATE_DETAILS

Field	Notes
BASELINE_NAME	Baseline name
BASELINE_ID	Unique ID generated for this baseline by the Update Manager server
BASELINE_VERSION	History about when the baseline was changed (old version remains in the database)
TYPE	Baseline type: virtual machine or host
TARGET_COMPONENT	Type of targets this baseline applies to: virtual machine or host
BASELINE_UPDATE_TYPE	Baseline type: fixed or dynamic

Table 13-15. VUMV_BASELINE_UPDATE_DETAILS (Continued)

Field	Notes
UPDATE_METAUID	Update meta ID
TITLE	Update title
SEVERITY	Update severity: Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
ID	Unique ID generated by the database: UPDATE_ID for updates and patches; RELEASE_ID for host upgrades;

VUMV_ENTITY_SCAN_RESULTS

This database view contains status history of a particular entity for an update.

Table 13-16. VUMV_ENTITY_SCAN_RESULTS

Field	Notes
SCANH_ID	Unique ID of the scan, generated by the database
ENTITY_UID	Entity unique ID (a managed object ID assigned by vCenter Server)
SCAN_START_TIME	Start time of the scan process
SCAN_END_TIME	End time of the scan process
UPDATE_METAUID	Update meta unique ID
UPDATE_TITLE	Update title
UPDATE_SEVERITY	Update severity: Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
ENTITY_STATUS	Status of the entity regarding the update: Missing, Installed, Not Applicable, Unknown, Staged, Conflict, ObsoletedByHost, MissingPackage, NotInstallable, NewModule, UnsupportedUpgrade, and IncompatibleHardware

VUMV_VMTOOLS_SCAN_RESULTS

This database view contains information about the latest results for VMware Tools scan.

Table 13-17. VUMV_VMTOOLS_SCAN_RESULTS

Field	Notes
SCANH_ID	Unique ID of the scan, generated by the database
ENTITY_UID	Entity unique ID (a managed object ID assigned by vCenter Server)
SCAN_START_TIME	Start time of the scan process
SCAN_END_TIME	End time of the scan process
ENTITY_STATUS	Status of the entity against the latest VMware Tools version

VUMV_VMHW_SCAN_RESULTS

This database view contains information about the latest results for virtual machine hardware scan.

Table 13-18. VUMV_VMHW_SCAN_RESULTS

Field	Notes
SCANH_ID	Unique ID of the scan, generated by the database
ENTITY_UID	Entity unique ID (a managed object ID assigned by vCenter Server)
SCAN_START_TIME	Start time of the scan process
SCAN_END_TIME	End time of the scan process
VM_HW_VERSION	Virtual machine hardware version
HOST_HW_VERSION	Hardware version recommended on the host